

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-293726

(43)Date of publication of application : 04.11.1998

(51)Int.Cl.

G06F 12/14
G09C 1/00
G11B 20/10
H04L 9/08
H04L 9/10

(21)Application number : 09-102288

(71)Applicant : TOSHIBA CORP

(22)Date of filing : 18.04.1997

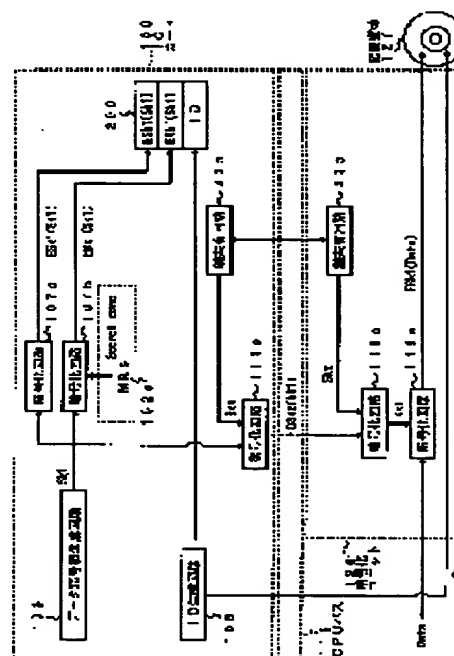
(72)Inventor : KATO TAKEHISA
ENDO NAOKI
TANAKA SEKIO
YOSHIDA NOBUHIRO

(54) EXTERNAL STORAGE DEVICE, CIPHERING UNIT DEVICE, DECODING UNIT DEVICE, CIPHERING SYSTEM, DECODING SYSTEM, CIPHERING METHOD AND DECODING METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To prevent unauthorized copying by a third person by respectively ciphering a data ciphering key for ciphering data by a prescribed master key and the data ciphering key itself and then recording it inside an external storage device corresponding to identification information imparted to the data.

SOLUTION: The identification information ID of the data of a ciphering object is generated in this external storage device (IC card 100) and the data ciphering key Sk1 used for the ciphering of the data is generated. Then, the identification information ID, the data ciphering key Sk1 respectively ciphered by the plural master keys stored in the form of being kept secret from the outside and the data ciphering key ciphered by the data ciphering key Sk1 itself are recorded inside the device in correspondence and the data ciphering key Sk1 is safely reported from the IC card 100 through the CPU bus 116 of a computer to this ciphering unit 126 without being obtained from the outside. In the ciphering unit device 126, the data are ciphered by using the data ciphering key Sk1.



LEGAL STATUS

[Date of request for examination]

11.09.2000

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(51)Int.Cl.⁸
 G 0 6 F 12/14
 G 0 9 C 1/00
 G 1 1 B 20/10
 H 0 4 L 9/08
 9/10

識別記号

3 2 0

6 6 0

F I

G 0 6 F 12/14

G 0 9 C 1/00

G 1 1 B 20/10

H 0 4 L 9/00

3 2 0 B

6 6 0 A

H

6 0 1 A

6 2 1 A

審査請求 未請求 請求項の数12 O L (全 34 頁)

(21)出願番号 特願平9-102288

(22)出願日 平成9年(1997)4月18日

(71)出願人 000003078

株式会社東芝

神奈川県川崎市幸区堀川町72番地

(72)発明者 加藤 岳久

神奈川県川崎市幸区小向東芝町1番地 株式会社東芝研究開発センター内

(72)発明者 遠藤 直樹

神奈川県川崎市幸区小向東芝町1番地 株式会社東芝研究開発センター内

(72)発明者 田中 哲男

東京都青梅市末広町2丁目9番地 株式会社東芝青梅工場内

(74)代理人 弁理士 鈴江 武彦 (外6名)

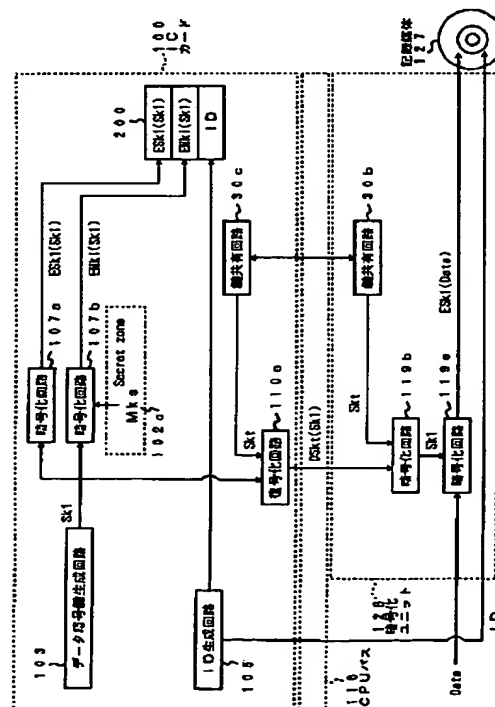
最終頁に続く

(54)【発明の名称】 外部記憶装置、暗号化ユニット装置、復号化ユニット装置、暗号化システム、復号化システム、暗号化方法及び復号化方法

(57)【要約】

【課題】 第三者による不正なコピーを防止することができる処理機能を有する外部記憶装置を提供すること。

【解決手段】 計算機のCPUバスを介さず入力したデータを所定の記録媒体に記録する前に暗号化する装置のためにデータ暗号化鍵を生成し記録するCPUバスに接続され使用される、処理機能を持つ外部記憶装置であって、予め定められた複数のマスター鍵を外部から秘匿した形で記憶するための手段と、暗号化対象のデータの識別情報を生成するための手段と、データの暗号化に用いるデータ暗号化鍵を生成するための手段と、識別情報とマスター鍵のうち所定数の鍵で夫々暗号化したデータ暗号化鍵とデータ暗号化鍵自身で暗号化したデータ暗号化鍵を対応付けて記録するための手段と、CPUバスを介して暗号化する装置にデータ暗号化鍵を外部から取得されことなく安全に伝えるための手段とを備える。



【特許請求の範囲】

【請求項1】 計算機のCPUバスを介さずに入力したデータを所定の記録媒体に記録する前に暗号化する装置のために、データ暗号化鍵を生成し記録する、計算機のCPUバスに接続されて使用される処理機能を有する外部記憶装置であって、

予め定められた複数のマスター鍵を外部から秘匿した形で記憶するための手段と、

暗号化対象となるデータの識別情報を生成するための手段と、

前記データの暗号化に用いるデータ暗号化鍵を生成するための手段と、

前記識別情報と、前記マスター鍵のうちの所定数のもので夫々暗号化したデータ暗号化鍵およびデータ暗号化鍵自身で暗号化したデータ暗号化鍵とを対応付けて記録するための手段と、

前記計算機のCPUバスを介して前記暗号化する装置に前記データ暗号化鍵を外部から取得されることなく安全に伝えるための手段とを備えたことを特徴とする外部記憶装置。

【請求項2】 自装置内に識別情報と対応して記録されている、前記予め定められた複数のマスター鍵のうちの所定数のもので夫々暗号化されたデータ暗号化鍵およびデータ暗号化鍵自身で暗号化されたデータ暗号化鍵のうちから、識別情報とこれに対応するデータ暗号化鍵で暗号化されたデータが記録された前記記録媒体から読み出され前記CPUバスを介して与えられた識別情報に対応するものを求めるための手段と、

前記予め定められた複数のマスター鍵を外部から秘匿した形で記憶するための手段を有し前記記録媒体から読み出され前記CPUバスを介して与えられた暗号化されたデータを復号する装置に、該CPUバスを介して、求められた前記予め定められた複数のマスター鍵のうちの所定数のもので夫々暗号化されたデータ暗号化鍵およびデータ暗号化鍵自身で暗号化されたデータ暗号化鍵を外部から取得されることなく安全に伝えるための手段とをさらに備えたことを特徴とする請求項1に記載の外部記憶装置。

【請求項3】 計算機のCPUバスを介さずに入力されたデータを、所定の記録媒体に記録する前に暗号化する暗号化ユニット装置であって、

暗号化対象となるデータの識別番号と該データの暗号化に用いるデータ暗号化鍵を生成し該識別番号と所定数のマスター鍵で夫々暗号化されたデータ暗号化鍵およびデータ暗号化鍵自身で暗号化されたデータ暗号化鍵とを対応付けて記録する装置から、前記計算機のCPUバスを介して、生成されたデータ暗号化鍵を外部から取得されることなく安全に受け取るための手段と、

受け取った前記データ暗号化鍵を用いて前記暗号化対象となるデータを暗号化するための手段とを備えたことを

特徴とする暗号化ユニット装置。

【請求項4】 暗号化されて所定の記録媒体に記録されたデータを復号する、計算機のCPUバスに接続されて使用される復号化ユニット装置であって、

予め定められた複数のマスター鍵を外部から秘匿した形で記憶するための手段と、

暗号化対象となったデータの識別番号と所定数のマスター鍵で夫々暗号化されたデータ暗号化鍵およびデータ暗号化鍵自身で暗号化されたデータ暗号化鍵とを対応付けて記録している装置から、前記計算機のCPUバスを介して、復号対象となる暗号化データの識別情報に対応する所定数のマスター鍵で夫々暗号化されたデータ暗号化鍵およびデータ暗号化鍵自身で暗号化されたデータ暗号化鍵を、外部から取得されることなく安全に受け取るための手段と、

自装置内に記憶されている前記複数のマスター鍵と受け取った前記所定数のマスター鍵で夫々暗号化されたデータ暗号化鍵およびデータ暗号化鍵自身で暗号化されたデータ暗号化鍵とをもとにして、データ暗号化鍵を求めるための手段と、

求められた前記データ暗号化鍵を復号鍵として、前記記録媒体から読み出され前記CPUバスを介して与えられた暗号化されたデータを復号するための手段とを備えたことを特徴とする復号化ユニット装置。

【請求項5】 前記データ暗号化鍵を求めるための手段は、前記受け取ったいずれかのマスター鍵で暗号化されたデータ暗号化鍵を自装置内に記録されているいずれかのマスター鍵を復号鍵として復号して得られる鍵候補と、この鍵候補を復号鍵として前記受け取ったデータ暗号化鍵自身で暗号化されたデータ暗号化鍵を復号して得られる鍵候補とが一致するものを探し求め、該一致が得られたときの鍵候補を求めるべきデータ暗号化鍵とするものであることを特徴とする請求項4に記載の復号化ユニット装置。

【請求項6】 前記記録媒体から読み出された暗号化されたデータを復号して得られたもとのデータに所定の変換処理を施した後に、前記計算機のCPUバスを介さず外部に出力するための手段とをさらに備えたことを特徴とする請求項4または5に記載の復号化ユニット装置。

【請求項7】 計算機のCPUバスに接続された処理機能を有する外部記憶装置と暗号化ユニット装置を用いてCPUバスを介さず外部から入力されたデータを所定の記録媒体に記録する前に暗号化する暗号化システムであって、

前記外部記憶装置は、

予め定められた複数のマスター鍵を外部から秘匿した形で記憶するための手段と、

暗号化対象となるデータの識別情報を生成するための手段と、

前記データの暗号化に用いるデータ暗号化鍵を生成する

ための手段と、

前記識別情報と、前記マスター鍵のうちの所定数のもので夫々暗号化したデータ暗号化鍵およびデータ暗号化鍵自身で暗号化したデータ暗号化鍵とを対応付けて記録するための手段と、

前記計算機のCPUバスを介して前記暗号化ユニット装置に前記データ暗号化鍵を外部から取得されることなく安全に伝えるための手段とを備え、

前記暗号化ユニット装置は、

前記外部記憶装置から前記計算機のCPUバスを介して、生成された前記データ暗号化鍵を外部から取得されることなく安全に受け取るための手段と、

受け取った前記データ暗号化鍵を用いて前記暗号化対象となるデータを暗号化するための手段とを備えたことを特徴とする暗号化システム。

【請求項8】前記伝えるための手段および前記受け取るための手段は、それぞれ、前記計算機のCPUバスを介した情報のやり取りにより協調して行われる所定の鍵共有手順により所定の一時鍵を外部から取得されることなく共有するための手段を備えるとともに、

前記伝えるための手段は、生成された前記データ暗号化鍵を共有した前記一時鍵で復号して出力するための手段を備え、

前記受け取るための手段は、与えられた前記一時鍵で復号されたデータ暗号化鍵を共有した前記一時鍵で暗号化するための手段を備えたことを特徴とする請求項7に記載の暗号化システム。

【請求項9】計算機のCPUバスに接続された処理機能を有する外部記憶装置と復号化ユニット装置を用いて所定の記録媒体に記録された暗号化されたデータを復号する復号化システムであって、

前記外部記憶装置は、

予め定められた複数のマスター鍵を外部から秘匿した形で記憶するための手段と、

暗号化の際に生成された暗号化対象となったデータの識別情報と前記マスター鍵のうちの所定数のもので夫々暗号化したデータ暗号化鍵およびデータ暗号化鍵自身で暗号化したデータ暗号化鍵とを対応付けて記録するための手段と、

自装置内に識別情報と対応して記録されている、前記予め定められた複数のマスター鍵のうちの所定数のもので夫々暗号化されたデータ暗号化鍵およびデータ暗号化鍵自身で暗号化されたデータ暗号化鍵のうちから、識別情報とこれに対応するデータ暗号化鍵で暗号化されたデータが記録された前記記録媒体から読み出され前記CPUバスを介して与えられた識別情報に対応するものを求めるための手段と、

求められた前記予め定められた複数のマスター鍵のうちの所定数のもので夫々暗号化されたデータ暗号化鍵およびデータ暗号化鍵自身で暗号化されたデータ暗号化鍵を

外部から取得されることなく安全に伝えるための手段とを備え、

前記復号化ユニット装置は、

予め定められた複数のマスター鍵を外部から秘匿した形で記憶するための手段と、

前記外部記憶装置から前記計算機のCPUバスを介して、前記所定数のマスター鍵で夫々暗号化されたデータ暗号化鍵およびデータ暗号化鍵自身で暗号化されたデータ暗号化鍵を、外部から取得されることなく安全に受け取るための手段と、

自装置内に記憶されている前記複数のマスター鍵と受け取った前記所定数のマスター鍵で夫々暗号化されたデータ暗号化鍵およびデータ暗号化鍵自身で暗号化されたデータ暗号化鍵とをもとにして、データ暗号化鍵を求めるための手段と、

求められた前記データ暗号化鍵を復号鍵として、前記記録媒体から読み出され前記CPUバスを介して与えられた暗号化されたデータを復号するための手段とを備えたことを特徴とする復号化システム。

【請求項10】前記伝えるための手段および前記受け取るための手段は、それぞれ、前記計算機のCPUバスを介した情報のやり取りにより協調して行われる所定の鍵共有手順により所定の一時鍵を外部から取得されることなく共有するための手段を備えるとともに、

前記伝えるための手段は、生成された前記データ暗号化鍵を共有した前記一時鍵で暗号化して出力するための手段を備え、

前記受け取るための手段は、与えられた前記一時鍵で復号されたデータ暗号化鍵を共有した前記一時鍵で復号するための手段を備えたことを特徴とする請求項9に記載の復号化システム。

【請求項11】計算機のCPUバスに接続された処理機能を有する外部記憶装置と暗号化ユニット装置を用いてCPUバスを介さずに外部から入力されたデータを所定の記録媒体に記録する前に暗号化する暗号化方法であって、

前記外部記憶装置にて、暗号化対象となるデータの識別情報を生成するとともに、該データの暗号化に用いるデータ暗号化鍵を生成し、該識別情報と、外部から秘匿した形で記憶された予め定められた複数のマスター鍵のうちの所定数のもので夫々暗号化したデータ暗号化鍵およびデータ暗号化鍵自身で暗号化したデータ暗号化鍵とを対応付けて自装置内の所定の記録領域に記録し、

前記外部記憶装置から前記計算機のCPUバスを介して前記暗号化ユニット装置に前記データ暗号化鍵を外部から取得されることなく安全に伝え、

前記暗号化ユニット装置にて、受け取った前記データ暗号化鍵を用いて前記暗号化対象となるデータを暗号化することを特徴とする暗号化方法。

【請求項12】計算機のCPUバスに接続された処理機

能を有する外部記憶装置と復号化ユニット装置を用いて所定の記録媒体に記録された暗号化されたデータを復号する復号化方法であって、

前記外部記憶装置にて、暗号化の際に生成され自装置内の所定の記憶領域に、暗号化対象となったデータの識別情報と対応付けられて記録されている、外部から秘匿した形で自装置内に記憶された予め定められた複数のマスター鍵のうちの所定数のもので夫々暗号化されたデータ暗号化鍵およびデータ暗号化鍵自身で暗号化されたデータ暗号化鍵のうちから、識別情報とこれに対応するデータ暗号化鍵で暗号化されたデータが記録された前記記録媒体から読み出され前記CPUバスを介して与えられた識別情報に対応するものを求め、

前記外部記憶装置から前記計算機のCPUバスを介して前記復号化ユニット装置に、求められた前記予め定められた複数のマスター鍵のうちの所定数のもので夫々暗号化されたデータ暗号化鍵およびデータ暗号化鍵自身で暗号化したデータ暗号化鍵を外部から取得されることなく安全に伝え、

前記復号化ユニット装置にて、外部から秘匿した形で自装置内に記憶されている予め定められた複数のマスター鍵と受け取った前記所定数のマスター鍵で夫々暗号化されたデータ暗号化鍵およびデータ暗号化鍵自身で暗号化されたデータ暗号化鍵とをもとにして、データ暗号化鍵を求め、

求められた前記データ暗号化鍵を復号鍵として、前記記録媒体から読み出され前記CPUバスを介して与えられた暗号化されたデータを復号することを特徴とする復号化方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、デジタル化された文書、音声、画像、プログラムなどのデータをネットワークを介して通信を行うシステムあるいは前記デジタルデータを記録保存し、読み出しするシステムのための外部記憶装置、暗号化ユニット装置、復号化ユニット装置、暗号化システム、復号化システム、暗号化方法及び復号化方法に関する。

【0002】

【従来の技術】現在、計算機が広範に普及しており、種々の分野で情報を電子化して処理し、あるいは情報を電子化して記録装置に保存することが通常行われるようになっている。また、ネットワーク環境も益々整ってきており、情報を電子化して通信することも通常行われるようになってきている。さらには、文書情報だけでなく、音声や画像などのデータを電子化して扱う技術も急速に進歩してきている。

【0003】ところで、電子化して扱う情報には、もちろん企業秘密や個人情報のように秘匿性を要する情報が含まれる。また、著作権に係る情報のように扱いに注意

を要する情報も含まれる。

【0004】そこで、情報を電子化して扱う際に、暗号化を行っておき、正当な者だけがこれを復号できるようにする技術が良く使われている。

【0005】例えば、データを暗号化して記録媒体に保存し、また記録媒体から暗号化データを読み出して復号し元のデータを取り出す暗号システムでは、予め暗号化と復号に用いる秘密鍵を定めておき、この秘密鍵を用いて保存、読み出しが行われる。このシステムによれば、秘密鍵を用いることができる者だけが保存された暗号化データを復号することができ、秘密鍵が解読されない限り、秘密鍵を用いることができない第三者が暗号化されたデータを不正に解読することはできない。

【0006】

【発明が解決しようとする課題】しかしながら、上記システムでは、もし第三者の不正な攻撃により秘密鍵が解読されると、すべての暗号化データが解読されるばかりでなく、解読により得たデータ（プレーンデータ）を自由にコピーすることが可能となってしまう。

【0007】また、秘密鍵が解読されなくても、他の暗号化システムにも同一の秘密鍵を内蔵するような場合には、暗号化データをそのままコピーすることにより、簡単に海賊版の作成ができてしまう。

【0008】さらに、秘密鍵が暴かれたことが発覚した場合、該当する暗号化システムの秘密鍵を更新する必要があるが複雑であるだけでなく、秘密鍵の更新後には当該暴かれた秘密鍵が復号にも使用できなくなるような更新形態をとるシステムにおいては、秘密鍵の更新後は当該暴かれた秘密鍵で暗号化されていたデータを復号することができなくなり、正当な者も元の内容を得ることができなくなってしまう不具合がある。

【0009】本発明は、上記事情を考慮してなされたものであり、第三者による不正なコピーを防止することができる外部記憶装置、暗号化ユニット装置、復号化ユニット装置、暗号化システム、復号化システム、暗号化方法及び復号化方法を提供することを目的とする。

【0010】また、本発明は、第三者が鍵情報を取得しあるいは暗号化データを解読することを困難にする外部記憶装置、暗号化ユニット装置、復号化ユニット装置、暗号化システム、復号化システム、暗号化方法及び復号化方法を提供することを目的とする。

【0011】さらに、本発明は、鍵情報の更新手続きを不要とする外部記憶装置、暗号化ユニット装置、復号化ユニット装置、暗号化システム、復号化システム、暗号化方法及び復号化方法を提供することを目的とする。

【0012】

【課題を解決するための手段】本発明は、計算機のCPUバスを介さずに入力したデータ（デジタル化されたデータ；例えば、文書、音声、画像、プログラムなど）を所定の記録媒体に記録する前に暗号化する装置のため

に、データ暗号化鍵を生成し記録する、計算機のCPUバスに接続されて使用される処理機能を有する外部記憶装置（例えば、ICカード）であって、予め定められた複数のマスター鍵を外部から秘匿した形で記憶するための手段と、暗号化対象となるデータの識別情報を生成するための手段と、前記データの暗号化に用いるデータ暗号化鍵を生成するための手段と、前記識別情報と、前記マスター鍵のうちの所定数のもの（例えば、任意に選んだ1つのマスター鍵、あるいは任意に選んだ複数のマスター鍵、あるいは全てのマスター鍵）で夫々暗号化したデータ暗号化鍵およびデータ暗号化鍵自身で暗号化したデータ暗号化鍵とを対応付けて記録するための手段と、前記計算機のCPUバスを介して前記暗号化する装置に前記データ暗号化鍵を外部から取得されることなく安全に伝えるための手段とを備えたことを特徴とする。

【0013】本発明は、上記構成において、自装置内に識別情報と対応して記録されている、前記予め定められた複数のマスター鍵のうちの所定数のもので夫々暗号化されたデータ暗号化鍵およびデータ暗号化鍵自身で暗号化されたデータ暗号化鍵のうちから、識別情報とこれに対応するデータ暗号化鍵で暗号化されたデータが記録された前記記録媒体から読み出され前記CPUバスを介して与えられた識別情報に対応するものを求めるための手段と、前記予め定められた複数のマスター鍵を外部から秘匿した形で記憶するための手段を有し前記記録媒体から読み出され前記CPUバスを介して与えられた暗号化されたデータを復号する装置に、該CPUバスを介して、求められた前記予め定められた複数のマスター鍵のうちの所定数のもので夫々暗号化されたデータ暗号化鍵およびデータ暗号化鍵自身で暗号化されたデータ暗号化鍵を外部から取得されることなく安全に伝えるための手段とをさらに備えたことを特徴とする。

【0014】本発明は、計算機のCPUバスを介さずに入力されたデータを、所定の記録媒体に記録する前に暗号化する暗号化ユニット装置であって、暗号化対象となるデータの識別番号と該データの暗号化に用いるデータ暗号化鍵を生成し該識別番号と所定数のマスター鍵で夫々暗号化されたデータ暗号化鍵およびデータ暗号化鍵自身で暗号化されたデータ暗号化鍵とを対応付けて記録する装置から、前記計算機のCPUバスを介して、生成されたデータ暗号化鍵を外部から取得されることなく安全に受け取るための手段と、受け取った前記データ暗号化鍵を用いて前記暗号化対象となるデータを暗号化するための手段とを備えたことを特徴とする。本発明は、暗号化されて所定の記録媒体に記録されたデータを復号する、計算機のCPUバスに接続されて使用される復号化ユニット装置であって、予め定められた複数のマスター鍵を外部から秘匿した形で記憶するための手段と、暗号化対象となったデータの識別番号と所定数のマスター鍵で夫々暗号化されたデータ暗号化鍵およびデータ暗号化

鍵自身で暗号化されたデータ暗号化鍵とを対応付けて記録している装置から、前記計算機のCPUバスを介して、復号対象となる暗号化データの識別情報に対応する所定数のマスター鍵で夫々暗号化されたデータ暗号化鍵およびデータ暗号化鍵自身で暗号化されたデータ暗号化鍵を、外部から取得されることなく安全に受け取るための手段と、自装置内に記憶されている前記複数のマスター鍵と受け取った前記所定数のマスター鍵で夫々暗号化されたデータ暗号化鍵およびデータ暗号化鍵自身で暗号化されたデータ暗号化鍵とをもとにして、データ暗号化鍵を求めるための手段と、求められた前記データ暗号化鍵を復号鍵として、前記記録媒体から読み出され前記CPUバスを介して与えられた暗号化されたデータを復号するための手段とを備えたことを特徴とする。

【0015】好ましくは、前記データ暗号化鍵を求めるための手段は、前記受け取ったいずれかのマスター鍵で暗号化されたデータ暗号化鍵を自装置内に記録されているいずれかのマスター鍵を復号鍵として復号して得られる鍵候補と、この鍵候補を復号鍵として前記受け取ったデータ暗号化鍵自身で暗号化されたデータ暗号化鍵を復号して得られる鍵候補とが一致するものを探し求め、該一致が得られたときの鍵候補を求めるべきデータ暗号化鍵とするものである。

【0016】好ましくは、前記記録媒体から読み出された暗号化されたデータを復号して得られたもとのデータに所定の変換処理を施した後に、前記計算機のCPUバスを介さず外部に出力するための手段をさらに備えても良い。

【0017】本発明は、計算機のCPUバスに接続された処理機能を有する外部記憶装置と暗号化ユニット装置を用いてCPUバスを介さず外部から入力されたデータを所定の記録媒体に記録する前に暗号化する暗号化システムであって、前記外部記憶装置は、予め定められた複数のマスター鍵を外部から秘匿した形で記憶するための手段と、暗号化対象となるデータの識別情報を生成するための手段と、前記データの暗号化に用いるデータ暗号化鍵を生成するための手段と、前記識別情報と、前記マスター鍵のうちの所定数のもので夫々暗号化したデータ暗号化鍵およびデータ暗号化鍵自身で暗号化したデータ暗号化鍵とを対応付けて記録するための手段と、前記計算機のCPUバスを介して前記暗号化ユニット装置に前記データ暗号化鍵を外部から取得されることなく安全に伝えるための手段とを備え、前記暗号化ユニット装置は、前記外部記憶装置から前記計算機のCPUバスを介して、生成された前記データ暗号化鍵を外部から取得されることなく安全に受け取るための手段と、受け取った前記データ暗号化鍵を用いて前記暗号化対象となるデータを暗号化するための手段とを備えたことを特徴とする。

【0018】好ましくは、前記伝えるための手段および

前記受け取るための手段は、それぞれ、前記計算機のCPUバスを介した情報のやり取りにより協調して行われる所定の鍵共有手順により所定の一時鍵を外部から取得されことなく共有するための手段を備えるとともに、前記伝えるための手段は、生成された前記データ暗号化鍵を共有した前記一時鍵で復号して出力するための手段を備え、前記受け取るための手段は、与えられた前記一時鍵で復号されたデータ暗号化鍵を共有した前記一時鍵で暗号化するための手段を備えるようにしても良い。

【0019】本発明は、計算機のCPUバスに接続された処理機能を有する外部記憶装置と復号化ユニット装置を用いて所定の記録媒体に記録された暗号化されたデータを復号する復号化システムであって、前記外部記憶装置は、予め定められた複数のマスター鍵を外部から秘匿した形で記憶するための手段と、暗号化の際に生成された暗号化対象となったデータの識別情報と前記マスター鍵のうちの所定数のもので夫々暗号化したデータ暗号化鍵およびデータ暗号化鍵自身で暗号化したデータ暗号化鍵とを対応付けて記録するための手段と、自装置内に識別情報と対応して記録されている、前記予め定められた複数のマスター鍵のうちの所定数のもので夫々暗号化されたデータ暗号化鍵およびデータ暗号化鍵自身で暗号化されたデータ暗号化鍵のうちから、識別情報とこれに対応するデータ暗号化鍵で暗号化されたデータが記録された前記記録媒体から読み出され前記CPUバスを介して与えられた識別情報に対応するものを求めるための手段と、求められた前記予め定められた複数のマスター鍵のうちの所定数のもので夫々暗号化されたデータ暗号化鍵およびデータ暗号化鍵自身で暗号化されたデータ暗号化鍵を外部から取得されことなく安全に伝えるための手段とを備え、前記復号化ユニット装置は、予め定められた複数のマスター鍵を外部から秘匿した形で記憶するための手段と、前記外部記憶装置から前記計算機のCPUバスを介して、前記所定数のマスター鍵で夫々暗号化されたデータ暗号化鍵およびデータ暗号化鍵自身で暗号化されたデータ暗号化鍵を、外部から取得されことなく安全に受け取るための手段と、自装置内に記憶されている前記複数のマスター鍵と受け取った前記所定数のマスター鍵で夫々暗号化されたデータ暗号化鍵およびデータ暗号化鍵自身で暗号化されたデータ暗号化鍵とをもとにして、データ暗号化鍵を求めるための手段と、求められた前記データ暗号化鍵を復号鍵として、前記記録媒体から読み出され前記CPUバスを介して与えられた暗号化されたデータを復号するための手段とを備えたことを特徴とする。

【0020】好ましくは、前記伝えるための手段および前記受け取るための手段は、それぞれ、前記計算機のCPUバスを介した情報のやり取りにより協調して行われる所定の鍵共有手順により所定の一時鍵を外部から取得されことなく共有するための手段を備えるとともに、

前記伝えるための手段は、生成された前記データ暗号化鍵を共有した前記一時鍵で暗号化して出力するための手段を備え、前記受け取るための手段は、与えられた前記一時鍵で復号されたデータ暗号化鍵を共有した前記一時鍵で復号するための手段を備えるようにしても良い。

【0021】好ましくは、前記データ暗号化鍵を求めるための手段は、前記受け取ったいずれかのマスター鍵で暗号化されたデータ暗号化鍵を自装置内に記録されているいずれかのマスター鍵を復号鍵として復号して得られる鍵候補と、この鍵候補を復号鍵として前記受け取ったデータ暗号化鍵自身で暗号化されたデータ暗号化鍵を復号して得られる鍵候補とが一致するものを探し求め、該一致が得られたときの鍵候補を求めるべきデータ暗号化鍵とするものである。

【0022】好ましくは、前記記録媒体から読み出された暗号化されたデータを復号して得られたもとのデータに所定の変換処理を施した後に、前記計算機のCPUバスを介さずに外部に出力するための手段をさらに備えても良い。

【0023】本発明は、計算機のCPUバスに接続された処理機能を有する外部記憶装置と暗号化ユニット装置を用いてCPUバスを介さずに外部から入力されたデータを所定の記録媒体に記録する前に暗号化する暗号化方法であって、前記外部記憶装置にて、暗号化対象となるデータの識別情報を生成するとともに、該データの暗号化に用いるデータ暗号化鍵を生成し、該識別情報と、外部から秘匿した形で記憶された予め定められた複数のマスター鍵のうちの所定数のもので夫々暗号化したデータ暗号化鍵およびデータ暗号化鍵自身で暗号化したデータ暗号化鍵とを対応付けて自装置内の所定の記録領域に記録し、前記外部記憶装置から前記計算機のCPUバスを介して前記暗号化ユニット装置に前記データ暗号化鍵を外部から取得されことなく安全に伝え、前記暗号化ユニット装置にて、受け取った前記データ暗号化鍵を用いて前記暗号化対象となるデータを暗号化することを特徴とする。

【0024】本発明は、計算機のCPUバスに接続された処理機能を有する外部記憶装置と復号化ユニット装置を用いて所定の記録媒体に記録された暗号化されたデータを復号する復号化方法であって、前記外部記憶装置にて、暗号化の際に生成され自装置内の所定の記憶領域に、暗号化対象となったデータの識別情報と対応付けられて記録されている、外部から秘匿した形で自装置内に記憶された予め定められた複数のマスター鍵のうちの所定数のもので夫々暗号化されたデータ暗号化鍵およびデータ暗号化鍵自身で暗号化されたデータ暗号化鍵のうちから、識別情報とこれに対応するデータ暗号化鍵で暗号化されたデータが記録された前記記録媒体から読み出され前記CPUバスを介して与えられた識別情報に対応するものを求め、前記外部記憶装置から前記計算機のCP

Uバスを介して前記復号化ユニット装置に、求められた前記予め定められた複数のマスター鍵のうちの所定数のもので夫々暗号化されたデータ暗号化鍵およびデータ暗号化鍵自身で暗号化されたデータ暗号化鍵を外部から取得されることなく安全に伝え、前記復号化ユニット装置にて、外部から秘匿した形で自装置内に記憶されている予め定められた複数のマスター鍵と受け取った前記所定数のマスター鍵で夫々暗号化されたデータ暗号化鍵およびデータ暗号化鍵自身で暗号化されたデータ暗号化鍵とをもとにして、データ暗号化鍵を求め、求められた前記データ暗号化鍵を復号鍵として、前記記録媒体から読み出され前記CPUバスを介して与えられた暗号化されたデータを復号することを特徴とする。

【0025】本発明によれば、データを暗号化したデータ暗号化鍵を所定のマスター鍵とデータ暗号化鍵自身でそれぞれ暗号化した上で、データに付与した識別情報に対応して外部記憶装置内に記録しておくことにより、この外部記憶装置と上記の暗号化に用いたマスター鍵を持つ復号化ユニットとを用いなければ復号を行うことができない。したがって、CPUバスから直接に他の記録媒体に記録するなどして記録媒体の複製を作って頒布しても他の者は復号をすることができない。

【0026】また、本発明によれば、暗号化されたデータ暗号化鍵を、例えば共有化した一時鍵を用いてさらに暗号化するなどして、外部記憶装置と暗号化ユニット装置との間あるいは外部記憶装置と復号化ユニット装置との間でCPUバスを介して共有するため、CPUバスからこれらの情報を記録することは無意味であるまた、本発明によれば、データを暗号化するデータ暗号化鍵自体も、またデータ暗号化鍵を共有化するために用いる一時鍵も、毎回変わるため、第3者により暗号を解読することは極めて困難である。

【0027】したがって、本発明によれば、第3者による不正なコピーを防止することが可能となる。

【0028】また、本発明によれば、鍵情報の更新手続きが不要となる。

【0029】

【発明の実施の形態】以下、図面を参照しながら発明の実施の形態を説明する。

【0030】本実施形態では、データを暗号化して記録媒体に記録し、また記録媒体から暗号化データを読み出し復号するシステムを例にとって説明する。

【0031】本実施形態では、暗号化の操作を E_x (x)と表す。ここで、 x は暗号化の対象となるデータであり、 y は暗号化に用いる暗号鍵である。また、復号化の操作を D_y (z)と表す。ここで、 z は復号化の対象となるデータであり、 y は復号化に用いる復号鍵である。

【0032】本実施形態では、あるデータをまず復号化し、その後、復号化されたデータを暗号化してもとのデ

ータに戻すことがある。これは、暗号の性質上、データの復号化に暗号化と同等の作用があることに基づいている。つまり、復号化したデータをもとに戻すためには復号化に用いた鍵がわからなければならず、鍵が判れば復号化したデータを暗号化することにより最初に復号化したデータが得られる。この操作は、暗号鍵を x としデータを y とすれば、

$$E_x (D_x (y)) = y$$

で表される。

【0033】本実施形態に係るシステムは、パーソナル・コンピュータなどの計算機（以下、PC）内に備えられたCPU（図示せず）のCPUバスに接続され、全体的な処理の流れの制御はプログラムで実現される。本実施形態では、データの入出力はCPUバス以外の例えばI/Oポート等を通じて行われるが、ディスクドライブ装置（図示せず）とユニットとの間、ユニットとユニットとの間でのデータ転送には、CPUバスが用いられる。従って、CPUバス上を流れるデータには、暗号化（あるいは暗号化に先だって行う復号化）を施している。

【0034】本実施形態は、概略的には、一纏まりのデータを暗号化する際に、データの暗号化に用いるデータ暗号化鍵 S_k1 と識別情報IDの対を生成し、IDと S_k1 を暗号化した形でICカード等の内部にデータベースとして記録しておくとともに、記録媒体にはIDと S_k1 で暗号化したデータを記録し、再生時には記録媒体から読み出したIDの情報をもとにデータベースから S_k1 を求め、 S_k1 を復号鍵として記録媒体に記録された暗号化データを復号するものである。

【0035】第1の実施形態ではCPUを介したICカード等とユニットと間で鍵を共有する1つの例を、第2、3の実施形態ではCPUを介したICカード等とユニット間で鍵を共有する他の1つの例を示す。また、第3の実施形態は第2の実施形態の構成の一部を簡素化したものである。

【0036】（第1の実施形態）図1は、本発明の第1の実施形態に係るデータの暗号化に用いるシステムの構成を示すブロック図である。なお、図1の鍵共有回路30b、30cの内部構成の一例を図2に示す。また、図3に本システムの暗号化の際の手順を、図4に鍵共有手順の一例を示す。

【0037】図5は、本発明の第1の実施形態に係るデータの復号に用いるシステムの構成を示すブロック図である。なお、図5の鍵共有回路30a、30cの内部構成の一例を図6に示す。また、図7に本システムの復号の際の手順を、図4に鍵共有手順の一例を示す。

【0038】図1に示すように、本実施形態に係るシステムは、処理機能を有する外部記憶装置（例えばICカード；以下ではICカードとする）100と暗号化ユニット126と復号化ユニット203を備えている。ま

た、ICカード100と暗号化ユニット126と復号化ユニット203は、PCのCPUバス116に接続されている。なお、ICカード100は使用時のみ接続し、それ以外では取り外して保管しておくのが望ましい。

【0039】また、CPUバス116にはディスクドライブ装置（図示せず）が接続されており、ディスクドライブ装置により記録媒体127への読み書きが行われる。

【0040】図1および図5に示すように、ICカード100は、暗号化に用いる部分として、データ暗号鍵生成回路103、ID生成回路105、暗号化回路107a、107b、復号化回路110eを備え、復号に用いる部分として、暗号化回路209b、209cを備え、暗号化と復号の両方に用いる部分としてID/鍵情報記憶回路200、鍵共有回路30cを備えている。上記構成部分は、独立した1つのICチップとして形成され、ICカード内に封止されているものとする。

【0041】暗号化ユニット126は、鍵共有回路30b、暗号化回路119b、119eを備えている。暗号化ユニット126は、独立した1つのICチップとして形成されるものとする。

【0042】復号化ユニット203は、鍵共有回路30a、復号化回路212b~212f、鍵判定回路（図示せず）を備えている。復号化ユニット203は、独立した1つのICチップとして形成されるものとする。

【0043】ICカード100内には、後述する複数のマスター鍵Mks（図中102c）が登録されている（作り込まれている）。

【0044】また、復号化ユニット203内には、ICカード100と同一の複数のマスター鍵Mks（図中102c）が登録されている（作り込まれている）。

【0045】なお、万一、マスター鍵が破られたことが発覚した場合、それ以降、ICカード100には、その破られたものを除いてマスター鍵が作り込まれる。ただし、復号化ユニット203については、その破られたものを除いてマスター鍵が作り込まれても良いし、そうしなくても良い。また、破られたマスター鍵が作り込まれているICカード100は、その破られたものを除いてマスター鍵が作り込まれている新しいもので更新するのが望ましい。ただし、復号化ユニット203は、破られたマスター鍵が作り込まれているものをそのまま使用しても構わない。なお、全体の制御は図示しない制御部が司るものとする。制御部は例えばプログラムを当該PCのCPUで実行することにより実現することができる。

【0046】データDataは、暗号化して記録する対象となる入力データであり、例えばPCのI/Oポートから入力される映像、音声、テキストなどのマルチメディア・データである。

【0047】IDは、本実施形態では、一纏まりのデータ毎（例えばタイトル毎）に与えられる識別番号であ

る。なお、IDは、ディスク毎に与えるようにしても良いし、ディスクの片面毎あるいは複数のディスクからなる組毎に与えるようにしても良いし、上記の一纏まりのデータをさらに細分化した部分毎（例えばチャプター毎あるいは曲毎など）に与えるようにしても良い。

【0048】Sk1は、データの暗号化および復号に用いるデータ暗号鍵（共通鍵暗号方式における共通鍵）であり、IDと対で生成される。

【0049】Mks（ $s=1\sim n$ 、 n は2以上の整数）は、マスター鍵（共通鍵暗号方式における共通鍵）の鍵束である。マスター鍵は、例えばメーカー毎に所定個数づつが割り当てられる。この場合、マスター鍵は、メーカー間で重複のないように割り当てられる。ここでは、一例として、 $s=1, \dots, 10$ （ $s=10$ ）とすると、Mk1, Mk2, ..., Mk10のマスター鍵が、ICカード100、復号化ユニット203のそれぞれに作り込まれる。

【0050】前述したように、マスター鍵の鍵束は、利用者が外部から取得できないように、ICカード内に封止されたチップ、復号化ユニットのチップそれぞれにおいて、利用者が意図的に取り出せないようにチップ内部の秘匿された領域に記録されているものとする。

【0051】Sk1は、CPUバス116上に情報を流す際に、該情報を暗号化あるいは復号（暗号化に先だって行う復号）するための、その都度変化する一時鍵（共通鍵暗号方式における共通鍵）である。

【0052】ID生成回路105は、ID番号を生成する。ID番号は、1から順番に発番するようにしても良いが、好ましくはランダムに発番する方が良い。後者の場合、生成されるIDが全て異なるようにするために、例えばID生成回路105を乱数発生器を用いて構成する方法が考えられる。なお、なお、重複発番する可能性のある乱数等を用いる場合には、生成したIDが既発番のものと同じであるかどうかチェックし、重複して発番されたことが分かったならば、そのIDは破棄し、別のIDを生成し直すようにすると好ましい。

【0053】データ暗号鍵生成回路103は、IDと対になるデータ暗号鍵Sk1を生成する。データ暗号鍵生成回路103は、例えば鍵長分の乱数発生器で構成しても良い。また、乱数を発生するにあたって、例えば時計（図示せず）からの時間情報を用いるようにしても良い。なお、全てのビットが0や1になる可能性のある乱数で鍵を生成する場合は、全てのビットが0や1になることがないようにチェック処理等をする必要がある。

【0054】ID/鍵情報記憶回路200は、後述するようにIDとEMki（Sk1）とESk1（Sk1）とを対応づけて記憶するためのものである（ここで、 i は $1\sim n$ のうちのいずれか）。

【0055】鍵共有回路30a、30b、30bは、少なくとも論理的に同一の構成を有し、後述する手順によ

り相手側回路と相互に情報の受け渡しをして同一の一時鍵（バス鍵） S_{kt} を生成し共有する。本実施形態では暗号化の際に暗号化ユニット126とICカード100が鍵共有回路30bと30cを用いて同一の一時鍵 S_{kt} を外部から知得されることなく安全に共有し、同様に復号の際に復号化ユニット203とICカード100が鍵共有回路30aと30cを用いて同一の一時鍵 S_{kt} を安全に共有する。鍵共有回路30a, 30b, 30cは外部からその内部の論理が解析されないようにICチップ内に作り込むものとする。

【0056】記録媒体127は、暗号化されたI/Oポートからの入力データを記録するためのものであり、例えばハードディスク、MO、FD、1回書き込み可能なCD、DVD-RAMなどを用いることが考えられる。

【0057】なお、ディスクドライブ装置内には、記録の際に変調、誤り訂正回路を行い、再生の際に復調、誤り訂正回路を行う変復調／誤り訂正回路が内蔵される場合がある。

【0058】また、本実施形態では、復号化ユニット203にはデジタルデータ $Data$ をアナログデータに変換するD/A変換回路が備えられ、復号化ユニット203からはアナログに変換されデータが出力されるものとする。また、デジタルデータ $Data$ が復号すべきものである場合にはこれを復号する復号回路をD/A変換回路の前に設けるものとする。例えばデジタルデータ $Data$ がMPEG方式で圧縮された画像データである場合に、MPEG復号回路を設けるものとする。また、種々の方式で圧縮等されたデータあるいは復号の必要ないデータのいずれも出力できるように、複数種類の復号回路を設け、これを適宜切替て使用し、あるいはこれらを使用しないように構成することも可能である。なお、復号化ユニット203からの出力は例えば画像としてディスプレイなどに表示される。

【0059】最初に、図1～図4を参照しながら、暗号化の際の手順について説明する。なお、図4におけるCPUはプログラムで実現した場合の制御部に相当し、ここではCPUすなわち制御部が手順の仲介を行っていることを示している。なお、制御部の仲介なしにユニット間で直接情報のやり取りを行うようにしても構わない。

【0060】まず、ICカード100をPCのカードスロットなど（図示せず）に差し込んでおく。また、記録媒体127がリムーバブルな媒体である場合には、これをディスクドライブ装置（図示せず）にセットしておく。

【0061】ステップS11では、ICカード100にて、ID生成回路105により入力データに対するIDが生成される。また、データ暗号鍵生成回路103により入力データを暗号化するための暗号鍵 S_{k1} が生成される。

【0062】ステップS12では、ICカード100に

て、暗号化回路107aにより S_{k1} 自身で S_{k1} を暗号化して、 ES_{k1} （ S_{k1} ）を得るとともに、暗号化回路107bにより、 n 個のマスター鍵 M_{ks} （ $s=1, \dots, n$ ）のうちから例えばランダムあるいは順番に選んだ1つ（これを M_{ki} とする）で S_{k1} を暗号化して、 EM_{ki} （ S_{k1} ）を得る。そして、得られたIDと ES_{k1} （ S_{k1} ）と EM_{ki} （ S_{k1} ）とを対応付けてICカード100内の記憶領域200に記録しておく。また、生成されたIDを記録媒体127に記録する。

【0063】なお、IDは、ICカード100からCPUバスを介して直接、ディスクドライブ装置に与えても良いし、ICカード100からCPUバスを介して暗号化ユニット126に与え、暗号化ユニット126からCPUバスを介してディスクドライブ装置に与えるようにしても良い。

【0064】ステップS13では、暗号化ユニット126とICカード100との間で鍵共有手順により一時鍵 S_{kt} を共有する。

【0065】ここでは、「日経エレクトロニクス No. 676 pp. 13-14 1996. 11. 18」に開示された技術を応用するものとする。

【0066】まず、本実施形態における鍵共有手順に用いる図2に示される鍵共有回路30b, 30cの構成について説明する。なお、ここでは図6に示す鍵共有回路30aについても併せて説明しておく。

【0067】鍵共有回路30aは、チャレンジ鍵生成回路31a、認証鍵生成回路33a、比較回路35a、バス鍵生成回路37aを備えている。同様に、鍵共有回路30bは、チャレンジ鍵生成回路31b、認証鍵生成回路33b、比較回路35b、バス鍵生成回路37bを備えている。同様に、鍵共有回路30cは、チャレンジ鍵生成回路31c、認証鍵生成回路33c、比較回路35c、バス鍵生成回路37cを備えている。

【0068】チャレンジ鍵生成回路31a, 31b, 31cは、例えば乱数生成アルゴリズムを用いて、生成の都度変化するチャレンジ鍵を生成する。

【0069】認証鍵生成回路33a, 33b, 33cは、例えば一方向性関数を用いて、チャレンジ鍵から認証鍵を生成する。

【0070】比較回路35b, 35cは、2つの認証鍵が一致するか否かを比較する。

【0071】バス鍵生成回路37a, 37b, 37cは、例えば一方向性関数を利用して、2つの認証鍵からバス鍵、すなわち一時鍵を生成する。

【0072】認証鍵生成回路33aと認証鍵生成回路33bと認証鍵生成回路33cは、例えば同一のアルゴリズムを用いることにより、同一のチャレンジ鍵に対して同一の認証鍵を生成するものとする。

【0073】バス鍵生成回路37aとバス鍵生成回路3

7bとバス鍵生成回路37cは、例えば同一のアルゴリズムを用いることにより、同一の2つの認証鍵から同一のバス鍵を生成するものとする。

【0074】次に、図2、図4を参照しながら、暗号化ユニット126とICカード100との間で行われる鍵共有手順について説明する。

【0075】まず、鍵共有手順のフェイズ1では、暗号化ユニット126にて、チャレンジ鍵生成回路31bによりチャレンジ鍵(Challenge Key)1を生成し、これをICカード100にも伝える。次に、暗号化ユニット126の認証鍵生成回路33bとICカード100の認証鍵生成回路33cのそれぞれにて、チャレンジ鍵1をもとに認証鍵1(Key1)を生成し、またICカード100から暗号化ユニット126へ生成した認証鍵1を転送する。そして、暗号化ユニット126にて、比較回路35bにより、暗号化ユニット126とICカード100のそれぞれで生成された2つの認証鍵1を比較する。もし一致すれば次のフェイズ2に移行する。もし一致しなければ異常終了となる。

【0076】次に、フェイズ2では、ICカード100にて、チャレンジ鍵生成回路31cによりチャレンジ鍵(Challenge Key)2を生成し、これを暗号化ユニット126にも伝える。次に、ICカード100の認証鍵生成回路33cと暗号化ユニット126の認証鍵生成回路33bのそれぞれにて、チャレンジ鍵2をもとに認証鍵2(Key2)を生成し、また暗号化ユニット126からICカード100へ生成した認証鍵2を転送する。そして、ICカード100にて、比較回路35cにより、ICカード100と暗号化ユニット126のそれぞれで生成された2つの認証鍵2を比較する。もし一致すれば次のフェイズ3に移行する。もし一致しなければ異常終了となる。

【0077】そして、フェイズ3では、暗号化ユニット126のバス鍵生成回路37bとICカード100のバス鍵生成回路37cのそれぞれにて、認証鍵1および認証鍵2をもとにバス鍵(BUS Key)すなわち一時鍵Sk tを生成する。

【0078】これによって、暗号化ユニット126とICカード100との間で安全に一時鍵Sk tが共有化される。

【0079】ステップS14では、ICカード100から暗号化ユニット126へ、共有化した一時鍵Sk tを用いてデータ暗号鍵Sk 1を伝える。すなわち、まず、ICカード100にて、復号化回路110eによりSk tでSk 1を復号して、DSk t(Sk 1)を得る。次に、ICカード100から暗号化ユニット126へ、DSk t(Sk 1)を送る。そして、暗号化ユニット126にて、暗号化回路119bにより、Sk tでDSk t(Sk 1)を暗号化して、Sk 1を得る。

【0080】ステップS14では、暗号化ユニット11

8にて、暗号化回路105cにより、Sk 1を暗号鍵として用いて入力データDataを暗号化して、ESk 1(Data)を得る。

【0081】ステップS15では、暗号化ユニット126にて、暗号化回路119eにより、Sk 1を暗号鍵として用いて入力データDataを暗号化して、ESk 1(Data)を得る。

【0082】ステップS16では、ESk 1(Data)を記録媒体117に記録する。

【0083】なお、1つの記録媒体に複数のIDが格納される場合、IDとESk 1(Data)とを対応付けて格納する。

【0084】次に、図4～図7を参照しながら、復号の際の手順について説明する。

【0085】まず、ICカード100をPCのカードスロットなど(図示せず)に差し込んでおく。また、記録媒体127がリムーバブルな媒体である場合には、これをディスクドライブ装置(図示せず)にセットしておく。

【0086】ステップS21では、ステップS13と同様にして、復号化ユニット203とICカード100との間で鍵共有手順により一時鍵Sk tを共有する。

【0087】まず、鍵共有手順のフェイズ1では、復号化ユニット203にて、チャレンジ鍵生成回路31aによりチャレンジ鍵(Challenge Key)1を生成し、これをICカード100にも伝える。次に、復号化ユニット203の認証鍵生成回路33aとICカード100の認証鍵生成回路33cのそれぞれにて、チャレンジ鍵1をもとに認証鍵1(Key1)を生成し、またICカード100から復号化ユニット203へ生成した認証鍵1を転送する。そして、復号化ユニット203にて、比較回路35aにより、復号化ユニット203とICカード100のそれぞれで生成された2つの認証鍵1を比較する。もし一致すれば次のフェイズ2に移行する。もし一致しなければ異常終了となる。

【0088】次に、フェイズ2では、ICカード100にて、チャレンジ鍵生成回路31cによりチャレンジ鍵(Challenge Key)2を生成し、これを復号化ユニット203にも伝える。次に、ICカード100の認証鍵生成回路33cと復号化ユニット203の認証鍵生成回路33aのそれぞれにて、チャレンジ鍵2をもとに認証鍵2(Key2)を生成し、また復号化ユニット203からICカード100へ生成した認証鍵2を転送する。そして、ICカード100にて、比較回路35cにより、ICカード100と復号化ユニット203のそれぞれで生成された2つの認証鍵2を比較する。もし一致すれば次のフェイズ3に移行する。もし一致しなければ異常終了となる。

【0089】そして、フェイズ3では、復号化ユニット203のバス鍵生成回路37aとICカード100のバ

ス鍵生成回路37cのそれぞれにて、認証鍵1および認証鍵2をもとにバス鍵(BUS Key)すなわち一時鍵Sk tを生成する。

【0090】これによって、復号化ユニット203とICカード100との間で安全に一時鍵Sk tが共有化される。

【0091】ステップS22では、記録媒体127に記録されたIDをICカード100へ送る。

【0092】ステップS23では、ICカード100にて、送られたIDをもとに、記録領域200から、対応するEMk i (Sk 1)とESk 1 (Sk 1)を取り出す。ステップS24では、復号化ユニット203へEMk i (Sk 1)とESk 1 (Sk 1)を送ることによって、データ暗号鍵Sk 1を復号化ユニット203へ伝えるための処理が行われる。以下、この手順について詳しく説明する。

【0093】まず、暗号化回路209bにより、一時鍵Sk tでEMk i (Sk 1)を暗号化して、ESk t (EMk i (Sk 1))を得る。また、暗号化回路209bにより、一時鍵Sk tでESk 1 (Sk 1)を暗号化して、ESk t (ESk 1 (Sk 1))を得る。そして、ESk t (EMk i (Sk 1))とESk t (ESk 1 (Sk 1))をCPUバス116を通して復号化ユニット203へ送る。

【0094】次に、復号化ユニット203にて、復号化回路212bにより、一時鍵Sk tでESk t (EMk i (Sk 1))を復号して、EMk i (Sk 1)を得る。また、復号化回路212dにより、一時鍵Sk tでESk t (ESk 1 (Sk 1))を復号して、ESk 1 (Sk 1)を得る。

【0095】次に、マスター鍵を1つ選ぶ(これをMk pとする)。

【0096】選んだMk pを復号鍵として、復号化回路212cにより、EMk i (Sk 1)を復号し、DMk p (EMk i (Sk 1))=Sk aを得る。

【0097】次に、復号化回路212cの出力Sk aを暗号鍵として、復号化回路212eにより、ESk 1 (Sk 1)を復号し、DSk a (ESk 1 (Sk 1))=Sk bを得る。

【0098】次に、図示しない鍵判定回路により、Sk aとSk bとが一致するか否か調べる。ここで、マスター鍵Mk iがMk pであったならば、 $Sk a = DMk p (EMk i (Sk 1)) = Sk 1$ となり、従って、 $Sk b = DSk a (ESk 1 (Sk 1)) = DSk 1 (ESk 1 (Sk 1)) = Sk 1$ となり、ゆえに、 $Sk a = Sk b = Sk 1$

となる。

【0099】つまり、鍵判定回路により、Sk aとSk bとが一致することがわかった場合には、 $Mk i = Mk p$ 、かつ、 $Sk a = Sk b = Sk 1$ であり、この場合、復号化回路212eの出力(あるいは復号化回路212cの出力)は、復号化回路212fに伝えられる。

【0100】一方、鍵判定回路により、Sk aとSk bとが一致しないことがわかった場合には、 $Mk i \neq Mk p$ であり、ICカード100にてSk 1はこのMk pでは暗号化されておらず、それ以外のマスター鍵で暗号化されたことが判る。

【0101】以降は、Sk aとSk bとが一致するまで、復号に用いるマスター鍵Mk pを変更して、上記の手順を繰り返す。

【0102】以上のような手順を用いて、マスター鍵Mk iを復号化ユニット203側で特定することができるとともに、データ暗号鍵Sk 1をICカード100から暗号化ユニット126へ安全に伝えることが可能となる。

【0103】ステップS25では、記録媒体127に記録されたESk 1 (Data)を復号化ユニット203へ送る。

【0104】ステップS27では、復号化ユニット203にて、復号化回路212fにより、Sk 1を復号鍵としてESk 1 (Data)を復号し、もとの入力データを得る。

【0105】なお、復号対象となるデータの暗号化に用いたICカードと当該ICカード100とが相違するものである場合、ICカード100内に対応するIDとEMk i (Sk 1)とESk 1 (Sk 1)の組が登録されていないので、上記のステップS24にてMk iを特定することもSk 1を得ることもできず、結局、対象となる暗号化データを復号することはできない。言い換えると、本実施形態では、記録媒体127とこれに暗号化データを記録した際に用いたICカードをセットで用いてのみ復号を行うことができる。

【0106】本実施形態で示した手順は一例であり種々変形することが可能である。

【0107】例えば、図3において、ステップS13の一時鍵の共有は最初に行っても良い。また、ステップS11、S12のIDの生成、データベースへの登録、記録媒体への記録は、それぞれどのようなタイミングで行っても良い。また、ステップS14はステップS12より先に行っても良い。また、暗号化ユニット内にバッファがあればデータはどのようなタイミングで読み込んでも良い。また、すべてのデータを暗号化してから記録媒体に記録しても良いが、所定の単位ごとに暗号化と記録(あるいは読み込みと暗号化と記録)を繰り返し行っても良い。

【0108】また、例えば図7において、ステップS2

1の一時鍵の共有は最初に行わなくても良い。復号化ユニット内にバッファがあれば暗号化データはどのようなタイミングで読み込んでも良い。また、すべてのデータを復号してから出力しても良いが、所定の単位ごとに復号と出力（あるいは読み込みと復号と出力）を繰り返し行っても良い。

【0109】上記の暗号化回路や復号化回路で用いる暗号化方式は、すべての部分で同じものを用いても良いし、対になる暗号化回路と復号化回路の組ごとに、用いる暗号化方式を適宜決めても良い（すべて異なるようにすることも可能である）。

【0110】また、上記では暗号化回路や復号化回路は独立した回路として示したが、暗号化回路や復号化回路は暗号化方式が同じであればユニット内あるいはICカード内において1つまたは複数のもので兼用するように構成しても構わない。例えば、暗号化ユニット126において暗号化回路119bと119eの暗号化方式が同じであれば、それらを1つの回路で構成しても良い。また、例えば、復号化ユニット203において復号化回路212b～212fの暗号化方式がすべて同じであれば、それらを1つの回路で構成しても良いし、あるいは3つの回路（例えば、復号化回路212b、212dに共用する回路、復号化回路212c、212eに共用する回路、復号化回路212f）で構成しても良いし、その他にも種々の構成が可能である。また、復号化ユニット203において復号化回路212b～212eの暗号化方式が同じで復号化回路212fのみ相違するならば、例えば2つの回路で構成することも可能であり、あるいは3つあるいは4つの回路で構成することも可能である。また、ICカード100についても同様に、暗号化回路107a、107b、209b、209cの4つを適宜共通化することが可能である。

【0111】ところで、ステップS12では、ICカード100にて、暗号化回路107aによりSk1自身でSk1を暗号化して、ESk1(Sk1)を得るとともに、暗号化回路107bにより、n個のマスター鍵Mks(s=1, ..., n)のうちから例えばランダムあるいは順番に選んだ1つ（これをMkiとする）でSk1を暗号化して、EMki(Sk1)を求め、そして、IDとESk1(Sk1)とEMki(Sk1)とを対応付けてICカード100内の記憶領域200に記録しておいた。

【0112】ここで、万一、マスター鍵が破られたことが発覚し、その破られたものを除いてマスター鍵が作り込まれた復号化ユニット203に取り替えた場合、すでにICカード100に記憶されているEMki(Sk1)に対応するマスター鍵は復号化ユニット203内に存在しないので、対応する暗号化データを復号することができなくなる。

【0113】そこで、上記構成を拡張して、n個のマス

ター鍵のうちから例えばランダムあるいは順番に選んだm個($2 \leq m \leq n$)のマスター鍵で夫々Sk1を暗号化して、m個のEMki(Sk1)を求め、IDとESk1(Sk1)とm個のEMki(Sk1)をとを対応付けてICカード100内の記憶領域200に記録しておいても良い。

【0114】この場合、ステップS24において、復号化ユニット203にて、m個のEMki(Sk1)のうちの1つを選択し、ステップS24の処理を行い、復号化ユニット203内のすべてのマスター鍵を用いても鍵判定回路によりSkaとSkbとの一致が得られず、マスター鍵Mkiが特定できなかったならば、m個のEMki(Sk1)のうちの他の1つを選択し、ステップS24の処理を行う。そして、上記手順を、鍵判定回路によりSkaとSkbとの一致が得られるまで繰り返す。

【0115】このようにすれば、ICカード100内のm個のEMki(Sk1)のうちのいずれかに対応するマスター鍵が破られ、その破られたものを除いてマスター鍵が作り込まれた復号化ユニット203に取り替えた場合でも、m個のEMki(Sk1)のすべてに対応するマスター鍵が破られない限り、対応する暗号化データを復号することができるようになる。

【0116】本実施形態では、暗号化ユニットはPC内に例えば暗号化ボードとして組み込まれCPUバスに接続されるものであったが、暗号化ユニットはディスクドライブ装置内に内蔵されることもある。

【0117】（第2の実施形態）図8は、本発明の第2の実施形態に係るデータの暗号化に用いるシステムの構成を示すブロック図である。なお、図8の305の部分および303の部分の詳細と一時鍵生成回路117を図9に示す。また、この場合の動作の一例を図10のフローチャートに示す。

【0118】図11は、本発明の第2の実施形態に係るデータの復号に用いるシステムの構成を示すブロック図である。なお、図11の215の部分および213の部分の詳細と一時鍵生成回路210を図12に示す。また、この場合の動作の一例を図13のフローチャートに示す。

【0119】図8に示すように、本実施形態に係るシステムは、ICカード100と暗号化ユニット126と復号化ユニット203を備えている。また、ICカード100と暗号化ユニット126と復号化ユニット203は、PCのCPUバス116に接続されている。なお、ICカード100は使用時のみ接続し、それ以外では取り外して保管しておくのが望ましい。

【0120】また、CPUバス116にはディスクドライブ装置（図示せず）が接続されており、ディスクドライブ装置により記録媒体127への読み書きが行われる。

【0121】図8および図9に示すように、ICカード

100は、暗号化に用いる部分として、データ暗号鍵生成回路103、ID生成回路105、暗号化回路107a、107b、復号化回路110a~110f、一時鍵判定回路313を備え、復号に用いる部分として、暗号化回路209a~209d、一時鍵判定回路211を備え、暗号化と復号の両方に用いる部分としてID/鍵情報記憶回路200を備えている。上記構成部分は、独立した1つのICチップとして形成され、ICカード内に封止されているものとする。

【0122】なお、上記では一時鍵判定回路211と一時鍵判定回路313は異なる回路としてあるが、その代わりに一時鍵判定回路211と一時鍵判定回路313を1つの回路で兼用しても構わない。

【0123】暗号化ユニット126は、一時鍵生成回路117、暗号化回路119a~119g、鍵判定回路（図示せず）を備えている。暗号化ユニット126は、独立した1つのICチップとして形成されるものとする。

【0124】復号化ユニット203は、一時鍵生成回路210、復号化回路212a~212g、鍵判定回路（図示せず）を備えている。復号化ユニット203は、独立した1つのICチップとして形成されるものとする。

【0125】復号化ユニット203内には、後述する複数のマスター鍵Mks（図中102a）が登録されている（作り込まれている）。

【0126】また、暗号化ユニット126内には、復号化ユニット126と同一の複数のマスター鍵Mks（図中102b）が登録されている（作り込まれている）。

【0127】同様に、ICカード100内には、復号化ユニット126と同一の複数のマスター鍵Mks（図中102c）が登録されている（作り込まれている）。

【0128】なお、万一、マスター鍵が破られたことが発覚した場合、それ以降、ICカード100、暗号化ユニット126、復号化ユニット203には、その破られたものを除いてマスター鍵が作り込まれる。また、破られたマスター鍵が作り込まれているICカード100、暗号化ユニット126、復号化ユニット203は、その破られたものを除いてマスター鍵が作り込まれている新しいものに差し替えるのが望ましい。

【0129】なお、全体の制御は図示しない制御部が司るものとする。制御部は例えばプログラムを当該PCのCPUで実行することにより実現することができる。

【0130】データDataは、暗号化して記録する対象となる入力データであり、例えばPCのI/Oポートから入力される映像、音声、テキストなどのマルチメディア・データである。

【0131】IDは、本実施形態では、一纏まりのデータ毎（例えばタイトル毎）に与えられる識別番号である。なお、IDは、ディスク毎に与えるようにしても良

いし、ディスクの片面毎あるいは複数のディスクからなる組毎に与えるようにしても良いし、上記の一纏まりのデータをさらに細分化した部分毎（例えばチャプター毎あるいは曲毎など）に与えるようにしても良い。

【0132】Sk1は、データの暗号化および復号に用いるデータ暗号鍵（共通鍵暗号方式における共通鍵）であり、IDと対で生成される。

【0133】Mks（ $s=1\sim n$ 、 n は2以上の整数）は、マスター鍵（共通鍵暗号方式における共通鍵）の鍵束である。マスター鍵は、例えばメカ毎に所定個数づつが割り当てられる。この場合、マスター鍵は、メカ間で重複のないように割り当てられる。ここでは、一例として、 $s=1, \dots, 10$ （ $s=10$ ）とすると、Mk1、Mk2、 \dots 、Mk10のマスター鍵が、ICカード100、暗号化ユニット126、復号化ユニット203のそれぞれに作り込まれる。

【0134】前述したように、マスター鍵の鍵束は、利用者が外部から取得できないように、ICカード内に封止されたチップ、暗号化ユニットのチップ、復号化ユニットのチップそれぞれにおいて、利用者が意図的に取り出せないようにチップ内部の秘匿された領域に記録されているものとする。

【0135】Sk1は、CPUバス116上に情報を流す際に、該情報を暗号化あるいは復号（暗号化に先だつて行う復号）するための、その都度変化する一時鍵（共通鍵暗号方式における共通鍵）である。

【0136】ID生成回路105は、ID番号を生成する。ID番号は、1から順番に発番するようにしても良いが、好ましくはランダムに発番する方が良い。後者の場合、生成されるIDが全て異なるようにするために、例えばID生成回路105を乱数発生器を用いて構成する方法が考えられる。なお、重複発番する可能性のある乱数等を用いる場合には、生成したIDが既発番のものと同じであるかどうかチェックし、重複して発番されたことが分かったならば、そのIDは破棄し、別のIDを生成し直すようにすると好ましい。

【0137】データ暗号鍵生成回路103は、IDと対になるデータ暗号鍵Sk1を生成する。データ暗号鍵生成回路103は、例えば鍵長分の乱数発生器で構成しても良い。また、乱数を発生するにあたって、例えば時計（図示せず）からの時間情報を用いるようにしても良い。なお、全てのビットが0や1になる可能性のある乱数で鍵を生成する場合は、全てのビットが0や1になることがないようにチェック処理等をする必要がある。

【0138】ID/鍵情報記憶回路200は、後述するようにIDとEMki（Sk1）とESk1（Sk1）とを対応づけて記憶するためのものである（ここで、 i は1~ n のうちのいずれか）。

【0139】一時鍵生成回路117、210は、それぞれ一時鍵Sk1を生成するためのものであり、その都度

生成する。一時鍵生成回路117, 210夫々は、例えば鍵長分の乱数発生器で構成する方法が考えられる。また、乱数を発生するにあたって、例えば時計（図示せず）からの時間情報を用いるようにしても良い。なお、全てのビットが0や1になる可能性のある乱数で鍵を生成する場合は、全てのビットが0や1になることがないようにチェック処理等をする必要がある。

【0140】記録媒体127は、暗号化されたI/Oポートからの入力データを記録するためのものであり、例えばハードディスク、MO、FD、1回書き込み可能なCD、DVD-RAMなどを用いることが考えられる。

【0141】なお、ディスクドライブ装置内には、記録の際に変調、誤り訂正回路を行い、再生の際に復調、誤り訂正回路を行う変復調／誤り訂正回路が内蔵される場合がある。

【0142】また、本実施形態では、復号化ユニット203にはデジタルデータDataをアナログデータに変換するD/A変換回路が備えられ、復号化ユニット203からはアナログに変換されデータが出力されるものとする。また、デジタルデータDataが復号すべきものである場合にはこれを復号する復号回路をD/A変換回路の前に設けるものとする。例えばデジタルデータDataがMPEG方式で圧縮された画像データである場合に、MPEG復号回路を設けるものとする。また、種々の方式で圧縮等されたデータあるいは復号の必要ないデータのいずれも出力できるように、複数種類の復号回路を設け、これを適宜切替て使用し、あるいはこれらを使用しないように構成することも可能である。なお、復号化ユニット203からの出力は例えば画像としてディスプレイなどに表示される。

【0143】最初に、図8～図10を参照しながら、暗号化の際の手順について説明する。まず、ICカード100をPCのカードスロットなど（図示せず）に差し込んでおく。また、記録媒体127がリムーバブルな媒体である場合には、これをディスクドライブ装置（図示せず）にセットしておく。

【0144】ステップS31では、ICカード100にて、ID生成回路105により入力データに対するIDが生成される。また、データ暗号鍵生成回路103により入力データを暗号化するための暗号鍵Sk1が生成される。

【0145】ステップS32では、ICカード100にて、暗号化回路107aによりSk1自身でSk1を暗号化して、ESk1(Sk1)を得るとともに、暗号化回路107bにより、n個のマスター鍵Mks(s=1, ..., n)のうちから例えばランダムあるいは順番に選んだ1つ（これをMkiとする）でSk1を暗号化して、EMki(Sk1)を得る。そして、得られたIDとESk1(Sk1)とEMki(Sk1)とを対応付けてICカード100内の記憶領域200に記録してお

く。また、生成されたIDを記録媒体127に記録する。

【0146】なお、IDは、ICカード100からCPUバスを介して直接、ディスクドライブ装置に与えても良いし、ICカード100からCPUバスを介して暗号化ユニット126に与え、暗号化ユニット126からCPUバスを介してディスクドライブ装置に与えるようにしても良い。

【0147】ステップS33では、ICカード100内で生成したデータ暗号鍵Sk1をCPUバス116を介して復号化ユニット126へ送るために用いる一時鍵Sktを、暗号化ユニット126側にて一時鍵生成回路117により生成する。

【0148】ステップS34では、以下に示すような手順を用いて、暗号化ユニット126からICカード100へ、生成された一時鍵Sktを伝える。

【0149】Sktのプレインデータを取得されないように、Sktは、暗号化ユニット126内に記録されたマスター鍵Mks(s=1, ..., n)のうちのいずれか（これをMkhとする）で暗号化され、EMkh(Skt)としてCPUバス116を通してICカード100へ送られる。

【0150】ここで、もしマスター鍵が1つだけ存在するのであれば（これをMk0とする）、単に暗号化ユニット126にてMk0でSktを暗号化し、このEMk0(Skt)をICカード100へ送り、ICカード100にてMk0でEMk0(Skt)を復号することにより、Sktを取り出すことができるが、本実施形態では、複数のマスター鍵からなる鍵束のうちの使用したマスター鍵Mkhを直接的に指し示す識別情報は暗号化ユニット126からICカード100へ伝えないようにし、その代わりに、上記マスター鍵Mkhを特定可能とする情報を暗号化ユニット126からICカード100へ送り、ICカード100にて、Sktの暗号化に使用されたマスター鍵Mkhがn個のマスター鍵のうちのいずれであるかを特定するとともに、このマスター鍵の特定を通じてSktを得る。

【0151】以下、図9、図10を参照しながら、ステップS34のより詳しい手順について説明する。

【0152】まず、暗号化ユニット126にて、暗号化回路307aにより、n個のマスター鍵Mks(i=1, ..., n)のうちから例えばランダムあるいは順番に選んだ1つ（これをMkhとする）で一時鍵Sktを暗号化して、EMkh(Skt)を得る。また、暗号化回路119gにより、一時鍵Skt自身を暗号化鍵として用いてSktを暗号化して、ESkt(Skt)を得る。そして、EMkh(Skt)とESkt(Skt)を、CPUバス106を通してICカード100へ送る。

【0153】次に、ICカード100にて、まずマスタ

一鍵を1つ選ぶ(これをMkpとする)。

【0154】選んだMkpを復号鍵として、復号化回路110cにより、EMkh(Skt)を復号し、
 $DMkp(EMkh(Skt)) = Ska$
 を得る。

【0155】次に、復号化回路110cの出力Skaを復号鍵として、復号化回路110cにより、ESkt(Skt)を復号し、
 $DSka(ESkt(Skt)) = Skb$
 を得る。

【0156】次に、一時鍵判定回路313により、SkaとSkbとが一致するか否か調べる。ここで、暗号化ユニット126にてSktを暗号化したマスター鍵MkhがMkpであったならば、
 $Ska = DMkp(EMki(Skt)) = Skt$
 となり、従って、
 $Skb = DSka(ESkt(Skt)) = DSkt(ESkt(Skt)) = Skt$
 となり、ゆえに、
 $Ska = Skb = Skt$
 となる。

【0157】つまり、一時鍵判定回路313により、SkaとSkbとが一致することがわかった場合には、Mkh=Mkp、かつ、 $Ska = Skb = Skt$ であり、この場合、一時鍵判定回路313は $Ska = Skb = Skt$ を出力する。

【0158】一方、一時鍵判定回路313により、SkaとSkbとが一致しないことがわかった場合には、Mkh≠Mkpであり、暗号化ユニット126にてSktはこのMkpでは暗号化されておらず、それ以外のマスター鍵で暗号化されたことが判る。この場合、一時鍵判定回路313は出力をしない(あるいは一時鍵判定回路313の出力が復号化回路110d、110eには伝えられない)。

【0159】以降は、SkaとSkbとが一致するまで、復号に用いるマスター鍵Mkpを変更して、上記の手順を繰り返す。例えば、最初にMkpとしてMk1を用いて上記の手順を行ってSkaとSkbとが一致しなかった場合に、次にMk2へと更新して再び上記の手順を繰り返すのである。

【0160】以上のような手順を用いて、暗号化ユニット126にてどのマスター鍵を用いたのかをICカード100側で特定することができるとともに、暗号化ユニット126とICカード100との間で一時鍵Sktを安全に共有することが可能となる。

【0161】ステップS35では、上記のようにして共有化した一時鍵Sktを用いて、ICカード100内で生成したデータ暗号鍵Sk1をCPUバス116を介して暗号化ユニット126へ伝える。

【0162】なおここでは、ICカード100にてデー

タ暗号鍵Sk1を一時鍵Sktで復号化し、DSkt(Sk1)をICカード100から暗号化ユニット126に送り、暗号化ユニット126にてDSkt(Sk1)をSktで暗号化して、Sk1を得るのではなく、上記のSktを共有した手順を併用する。

【0163】まず、ICカード100にて、復号化回路110bにより、n個のマスター鍵Mks(s=1, ..., n)のうちから例えばランダムあるいは順番に選んだ1つ(これをMkjとする)でデータ暗号鍵Sk1を暗号化して、DMkj(Sk1)を得る。また、復号化回路110aにより、Sk1自身を復号鍵として用いてSk1を復号して、DSk1(Sk1)を得る。

【0164】次に、復号化回路110eにより、一時鍵SktでDMkj(Sk1)を復号して、DSkt(DMkj(Sk1))を得る。また、復号化回路110dにより、一時鍵SktでDSk1(Sk1)を復号して、DSkt(DSk1(Sk1))を得る。そして、DSkt(DMkj(Sk1))とDSkt(DSk1(Sk1))をCPUバス116を通して暗号化ユニット126へ送る。

【0165】次に、暗号化ユニット126にて、暗号化回路119bにより、一時鍵SktでDSkt(DMkj(Sk1))を暗号化して、DMkj(Sk1)を得る。また、暗号化回路119aにより、一時鍵SktでDSkt(DSk1(Sk1))を暗号化して、DSk1(Sk1)を得る。

【0166】ここで、ICカード100にて用いられたマスター鍵が、n個のうちのどのマスター鍵であったかは、暗号化ユニット126側ではわからない。そこで、前述したICカード100にてマスター鍵の特定を通じて一時鍵Sktを求める手順と同じ手順により、暗号化ユニット126にてマスター鍵の特定を通じてデータ暗号鍵Sk1を求める。

【0167】まず、暗号化ユニット126にて、マスター鍵を1つ選ぶ(これをMkpとする)。

【0168】選んだMkpを暗号鍵として、暗号化回路119cにより、DMkj(Sk1)を暗号化し、
 $EMkp(DMkj(Sk1)) = Ska$
 を得る。

【0169】次に、暗号化回路119cの出力Skaを暗号鍵として、暗号化回路119dにより、DSk1(Sk1)を暗号化し、
 $ESka(DSk1(Sk1)) = Skb$
 を得る。

【0170】次に、図示しない鍵判定回路により、SkaとSkbとが一致するか否か調べる。ここで、ICカード100にてSk1を復号したマスター鍵MkjがMkpであったならば、
 $Ska = EMkp(DMkj(Sk1)) = Sk1$
 となり、従って、

$S k b = E S k a (D S k 1 (S k 1)) = E S k 1$
 $(D S k 1 (S k 1)) = S k 1$

となり、ゆえに、

$S k a = S k b = S k 1$

となる。

【0171】つまり、鍵判定回路により、 $S k a$ と $S k b$ とが一致することがわかった場合には、 $M k j = M k p$ 、かつ、 $S k a = S k b = S k 1$ であり、この場合、暗号化回路119dの出力（あるいは暗号化回路119cの出力）は、暗号化回路119eに伝えられる。

【0172】一方、鍵判定回路により、 $S k a$ と $S k b$ とが一致しないことがわかった場合には、 $M k j \neq M k p$ であり、ICカード100にて $S k 1$ はこの $M k p$ では暗号化されておらず、それ以外のマスター鍵で復号されたことが判る。

【0173】以降は、 $S k a$ と $S k b$ とが一致するまで、暗号化に用いるマスター鍵 $M k p$ を変更して、上記の手順を繰り返す。

【0174】以上のような手順を用いて、ICカード100にてどのマスター鍵を用いたのかを暗号化ユニット126側で特定することができるとともに、ICカード100内にて生成されたデータ暗号鍵 $S k 1$ をICカード100から暗号化ユニット126へ安全に伝えることが可能となる。

【0175】ステップS36では、暗号化ユニット126にて、暗号化回路119eにより、 $S k 1$ を暗号鍵として用いて入力データ $D a t a$ を暗号化して、 $E S k 1 (D a t a)$ を得る。

【0176】ステップS37では、 $E S k 1 (D a t a)$ を記録媒体127に記録する。

【0177】なお、1つの記録媒体に複数のIDが格納される場合、IDと $E S k 1 (D a t a)$ とを対応付けて格納する。

【0178】次に、図11～図13を参照しながら、復号の際の手順について説明する。

【0179】。

【0180】まず、ICカード100をPCのカードスロットなど（図示せず）に差し込んでおく。また、記録媒体127がリムーバブルな媒体である場合には、これをディスクドライブ装置（図示せず）にセットしておく。

【0181】ステップS41では、ICカード100内の記憶領域200に格納された暗号化されたデータ暗号鍵 $S k 1$ をCPUバス116を介して復号化ユニット203へ送るために用いる一時鍵 $S k t$ を、復号化ユニット203側にて一時鍵生成回路210により生成する。

【0182】ステップS42では、先のステップS34にて用いた手順と同様の手順を利用して、復号化ユニット203からICカード100へ、生成された一時鍵 $S k t$ を伝える。

【0183】以下、図12、図13を参照しながら、ステップS42のより詳しい手順について説明する。

【0184】まず、復号化ユニット203にて、復号化回路212aにより、 n 個のマスター鍵 $M k s$ ($s = 1, \dots, n$)のうちのいずれか（これを $M k h$ とする）で一時鍵 $S k t$ を復号して、 $D M k h (S k t)$ を得る。また、復号化回路212gにより、一時鍵 $S k t$ 自身を暗号化鍵として用いて $S k t$ を暗号化して、 $D S k t (S k t)$ を得る。そして、 $D M k h (S k t)$ と $D S k t (S k t)$ を、CPUバス106を通してICカード100へ送る。

【0185】次に、ICカード100にて、まずマスター鍵を1つ選ぶ（これを $M k p$ とする）。

【0186】選んだ $M k p$ を暗号鍵として、暗号化回路209cにより、 $D M k h (S k t)$ を暗号化し、 $E M k p (D M k h (S k t)) = S k a$ を得る。

【0187】次に、暗号化回路209cの出力 $S k a$ を復号鍵として、暗号化回路209dにより、 $D S k t (S k t)$ を暗号化し、 $E S k a (D S k t (S k t)) = S k b$ を得る。

【0188】次に、一時鍵判定回路211により、 $S k a$ と $S k b$ とが一致するか否か調べる。ここで、暗号化ユニット126にて $S k t$ を暗号化したマスター鍵 $M k h$ が $M k p$ であったならば、

$S k a = E M k p (D M k h (S k t)) = S k t$

となり、従って、

$S k b = E S k a (D S k t (S k t)) = E S k t$
 $(D S k t (S k t)) = S k t$

となり、ゆえに、

$S k a = S k b = S k t$

となる。

【0189】つまり、一時鍵判定回路211により、 $S k a$ と $S k b$ とが一致することがわかった場合には、 $M k h = M k p$ 、かつ、 $S k a = S k b = S k t$ であり、この場合、一時鍵判定回路211は $S k a = S k b = S k t$ を出力する。

【0190】一方、一時鍵判定回路211により、 $S k a$ と $S k b$ とが一致しないことがわかった場合には、 $M k h \neq M k p$ であり、復号化ユニット203にて $S k t$ はこの $M k p$ では暗号化されておらず、それ以外のマスター鍵で復号されたことが判る。この場合、一時鍵判定回路211は出力をしない（あるいは一時鍵判定回路211の出力が復号化回路209b、209cには伝えられない）。

【0191】以降は、 $S k a$ と $S k b$ とが一致するまで、暗号化に用いるマスター鍵 $M k p$ を変更して、上記の手順を繰り返す。

【0192】以上のような手順を用いて、復号化ユニッ

ト203にてどのマスター鍵を用いたのかをICカード100側で特定することができるとともに、復号化ユニット203とICカード100との間で一時鍵Sk tを安全に共有することが可能となる。

【0193】ステップS43では、記録媒体127に記録されたIDをICカード200へ送る。

【0194】ステップS44では、ICカード100にて、送られたIDをもとに、記録領域200から、対応するEMk i (Sk 1)とESk 1 (Sk 1)を取り出す。ステップS45では、復号化ユニット126へEMk i (Sk 1)とESk 1 (Sk 1)を送ることによって、データ暗号鍵Sk 1を復号化ユニット126へ伝えるための処理が行われる。

【0195】ここでは、ステップS35にて用いた手順と同様の手順を利用して、ICカード100から復号化ユニット203へSk 1を伝える。

【0196】まず、暗号化回路209bにより、一時鍵Sk tでEMk i (Sk 1)を暗号化して、ESk t (EMk i (Sk 1))を得る。また、暗号化回路209bにより、一時鍵Sk tでESk 1 (Sk 1)を暗号化して、ESk t (ESk 1 (Sk 1))を得る。そして、ESk t (EMk i (Sk 1))とESk t (ESk 1 (Sk 1))をCPUバス116を通して復号化ユニット203へ送る。

【0197】次に、復号化ユニット203にて、復号化回路212bにより、一時鍵Sk tでESk t (EMk i (Sk 1))を復号して、EMk i (Sk 1)を得る。また、復号化回路212dにより、一時鍵Sk tでESk t (ESk 1 (Sk 1))を復号して、ESk 1 (Sk 1)を得る。

【0198】次に、マスター鍵を1つ選ぶ(これをMk pとする)。

【0199】選んだMk pを復号鍵として、復号化回路212cにより、EMk i (Sk 1)を復号し、DMk p (EMk i (Sk 1))=Sk aを得る。

【0200】次に、復号化回路212cの出力Sk aを暗号鍵として、復号化回路212eにより、ESk 1 (Sk 1)を復号し、

DSk a (ESk 1 (Sk 1))=Sk bを得る。

【0201】次に、図示しない鍵判定回路により、Sk aとSk bとが一致するか否か調べる。ここで、マスター鍵Mk iがMk pであったならば、

Sk a=DMk p (EMk i (Sk 1))=Sk 1

となり、従って、

Sk b=DSk a (ESk 1 (Sk 1))=DSk 1 (ESk 1 (Sk 1))=Sk 1

となり、ゆえに、

Sk a=Sk b=Sk 1

となる。

【0202】つまり、鍵判定回路により、Sk aとSk bとが一致することがわかった場合には、Mk i=Mk p、かつ、Sk a=Sk b=Sk 1であり、この場合、復号化回路212eの出力(あるいは復号化回路212cの出力)は、復号化回路212fに伝えられる。

【0203】一方、鍵判定回路により、Sk aとSk bとが一致しないことがわかった場合には、Mk i≠Mk pであり、ICカード100にてSk 1はこのMk pでは暗号化されておらず、それ以外のマスター鍵で暗号化されたことが判る。

【0204】以降は、Sk aとSk bとが一致するまで、復号に用いるマスター鍵Mk pを変更して、上記の手順を繰り返す。

【0205】以上のような手順を用いて、マスター鍵Mk iを復号化ユニット203側で特定することができるとともに、データ暗号鍵Sk 1をICカード100から暗号化ユニット126へ安全に伝えることが可能となる。

【0206】ステップS46では、記録媒体127に記録されたESk 1 (Data)を復号化ユニット203へ送る。

【0207】ステップS47では、復号化ユニット203にて、復号化回路212fにより、Sk 1を復号鍵としてESk 1 (Data)を復号し、もとの入力データを得る。

【0208】なお、復号対象となるデータの暗号化に用いたICカードと当該ICカード100とが相違するものである場合、ICカード100内に対応するIDとEMk i (Sk 1)とESk 1 (Sk 1)の組が登録されていないので、上記のステップS45にてMk iを特定することもSk 1を得ることもできず、結局、対象となる暗号化データを復号することはできない。言い換えると、本実施形態では、記録媒体127とこれに暗号化データを記録した際に用いたICカードをセットで用いてのみ復号を行うことができる。

【0209】本実施形態で示した手順は一例であり種々変形することが可能である。

【0210】例えば、図10において、ステップS13の一時鍵の共有は最初に行っても良い。また、ステップS31、S32のIDの生成、データベースへの登録、記録媒体への記録は、それぞれどのようなタイミングで行っても良い。また、ステップS35は、ステップS33あるいはS34より先に行っても良い。また、ステップS33はS32より先に行っても良い。また、暗号化ユニット内にバッファがあればデータはどのようなタイミングで読み込んでも良い。また、すべてのデータを暗号化してから記録媒体に記録しても良いが、所定の単位ごとに暗号化と記録(あるいは読み込みと暗号化と記録)を繰り返し行っても良い。

【0211】また、例えば図13において、ステップS41～ステップS45の順序は適宜入れ替えることが可能である。また、復号化ユニット内にバッファがあれば暗号化データはどのようなタイミングで読み込んでも良い。また、すべてのデータを復号してから出力しても良いが、所定の単位ごとに復号と出力（あるいは読み込みと復号と出力）を繰り返し行っても良い。

【0212】ところで、ステップS32では、ICカード100にて、暗号化回路107aによりSk1自身でSk1を暗号化して、ESk1(Sk1)を得るとともに、暗号化回路107bにより、n個のマスター鍵Mks(s=1, ..., n)のうちから例えばランダムあるいは順番に選んだ1つ（これをMkiとする）でSk1を暗号化して、EMki(Sk1)を求め、そして、IDとESk1(Sk1)とEMki(Sk1)とを対応付けてICカード100内の記憶領域200に記録しておいた。

【0213】ここで、万一、マスター鍵が破られたことが発覚し、その破られたものを除いてマスター鍵が作り込まれた復号化ユニット203に取り替えた場合、すでにICカード100に記憶されているEMki(Sk1)に対応するマスター鍵は復号化ユニット203内に存在しないので、対応する暗号化データを復号することができなくなる。

【0214】そこで、上記構成を拡張して、n個のマスター鍵のうちから例えばランダムあるいは順番に選んだm個(2≤m≤n)のマスター鍵で夫々Sk1を暗号化して、m個のEMki(Sk1)を求め、IDとESk1(Sk1)とm個のEMki(Sk1)とを対応付けてICカード100内の記憶領域200に記録しておいても良い。

【0215】この場合、ステップS45において、復号化ユニット203にて、m個のEMki(Sk1)のうちの1つを選択し、ステップS45の処理を行い、復号化ユニット203内のすべてのマスター鍵を用いても鍵判定回路によりSkaとSkbとの一致が得られず、マスター鍵Mkiが特定できなかったならば、m個のEMki(Sk1)のうちの他の1つを選択し、ステップS45の処理を行う。そして、上記手順を、鍵判定回路によりSkaとSkbとの一致が得られるまで繰り返す。

【0216】このようにすれば、ICカード100内のm個のEMki(Sk1)のうちのいずれかに対応するマスター鍵が破られ、その破られたものを除いてマスター鍵が作り込まれた復号化ユニット203に取り替えた場合でも、m個のEMki(Sk1)のすべてに対応するマスター鍵が破られない限り、対応する暗号化データを復号することができるようになる。

【0217】第1の実施形態と同様に、上記の暗号化回路や復号化回路で用いる暗号化方式は、すべての部分で同じものを用いても良いし、対になる暗号化回路と復号

化回路の組ごとに、用いる暗号化方式を適宜決めても良い（すべて異なるようにすることも可能である）。

【0218】また、第1の実施形態と同様に、暗号化回路や復号化回路は暗号化方式が同じであればユニット内あるいはICカード内において1つまたは複数のもので兼用するように構成しても構わない。

【0219】（第3の実施形態）次に、本発明の第3の実施形態について説明する。

【0220】本実施形態は、第3の実施形態において、ステップS35のデータ暗号鍵Sk1をICカード100から暗号化ユニット126へ伝えるための手順とそのためのICカード100と暗号化ユニット126の構成を簡略化したものであり、それ以外の点は先の実施形態と同様である。

【0221】すなわち、先の実施形態では、ステップS35においてSk1の復号（暗号化に先だって行う復号）には一時鍵Sk tといずれかのマスター鍵Mkjの2つを用いて2重の復号を行ったが、本実施形態では、Sk tのみ用いるようにしたものである。

【0222】したがって、本実施形態では、図8の構成から、暗号化ユニット126の暗号化回路119a, 119c, 119d、図示しない鍵判定回路と、ICカード100の復号回路110a, 110b, 110dを削除した構成になる。これを図14に示す。また、図10のフローチャートは、図15のようになり、ステップS35の部分だけが相違する。図9、図11～図13の構成は、本実施形態でも同様である。

【0223】以下では、ステップS65についてのみ説明する。

【0224】ステップS65では、まず、復号化回路110eにより、一時鍵Sk tでSk1を復号して、DSk t(Sk1)を得る。そして、DSk t(Sk1)をCPUバス116を通して暗号化ユニット126へ送る。

【0225】次に、暗号化ユニット126にて、暗号化回路119bにより、一時鍵Sk tでDSk t(Sk1)を暗号化して、Sk1を得る。

【0226】本発明は、上述した実施の形態に限定されるものではなく、その技術的範囲において種々変形して実施することができる。

【0227】

【発明の効果】本発明によれば、データを暗号化したデータ暗号化鍵を所定のマスター鍵とデータ暗号化鍵自身でそれぞれ暗号化した上で、データに付与した識別情報に対応して外部記憶装置内に記録しておくことにより、この外部記憶装置と上記の暗号化に用いたマスター鍵を持つ復号化ユニット装置とを用いなければ復号を行うことができない。したがって、CPUバスから直接に他の記録媒体に記録するなどして記録媒体の複製を作って頒布しても他の者は復号をすることができない。

【0228】また、本発明によれば、暗号化されたデータ暗号化鍵を、例えば共有化した一時鍵を用いてさらに暗号化するなどして、外部記憶装置と暗号化ユニット装置との間あるいは外部記憶装置と復号化ユニット装置との間でCPUバスを介して共有するため、CPUバスからこれらの情報を記録することは無意味であるまた、本発明によれば、データを暗号化するデータ暗号化鍵自体も、またデータ暗号化鍵を共有化するために用いる一時鍵も、毎回変わるため、第三者により暗号を解読することは極めて困難である。

【0229】したがって、本発明によれば、第三者による不正なコピーを防止することが可能となる。

【図面の簡単な説明】

【図1】本発明の第1の実施形態に係る暗号化に用いるシステムの構成を示すブロック図

【図2】図1の鍵共有回路の内部構成の一例を示す図

【図3】同実施形態における暗号化の際の手順を示すフローチャート

【図4】鍵共有手順の一例を示すフローチャート

【図5】同実施形態に係る復号に用いるシステムの構成を示すブロック図

【図6】図5の鍵共有回路の内部構成の一例を示す図

【図7】同実施形態における復号の際の手順を示すフローチャート

【図8】本発明の第2の実施形態に係る暗号化に用いるシステムの構成を示すブロック図

【図9】図8の鍵共有のための構成部分301、303の詳しい構成の一例を示す図

【図10】同実施形態における暗号化の際の手順を示すフローチャート

【図11】同実施形態に係る復号に用いるシステムの構成を示すブロック図

【図12】図11の鍵共有のための構成部分213、215の詳しい構成の一例を示す図

【図13】同実施形態における復号の際の手順を示すフローチャート

【図14】本発明の第3の実施形態に係る暗号化に用いるシステムの構成を示すブロック図

【図15】同実施形態における暗号化の際の手順を示すフローチャート

【符号の説明】

30a、30b、30c…鍵共有回路

31a、31b、31c…チャレンジ鍵生成回路

33a、33b、33c…認証鍵生成回路

35a、35b、35c…比較回路

37a、37b、37c…バス鍵生成回路

100…ICカード

102a～102c…マスター鍵の鍵束

103…データ暗号鍵生成回路

105…ID生成回路

107a、107b、119a～119g、209a～

209d…暗号化回路

110a～110f、212a～212g…復号化回路

116…CPUバス

117、210…一時鍵生成回路

126…暗号化ユニット

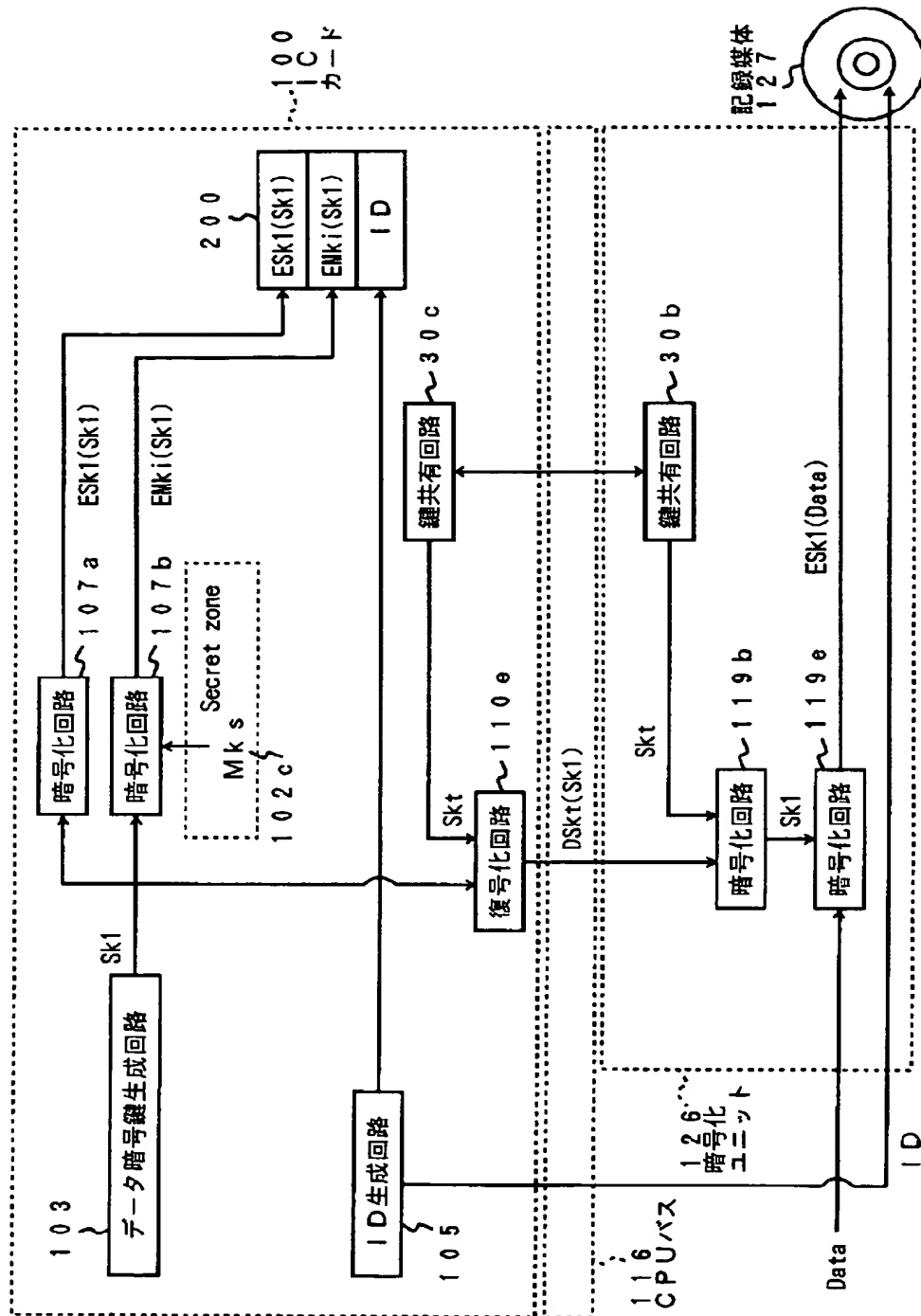
127…記録媒体

200…ID/鍵情報記憶回路

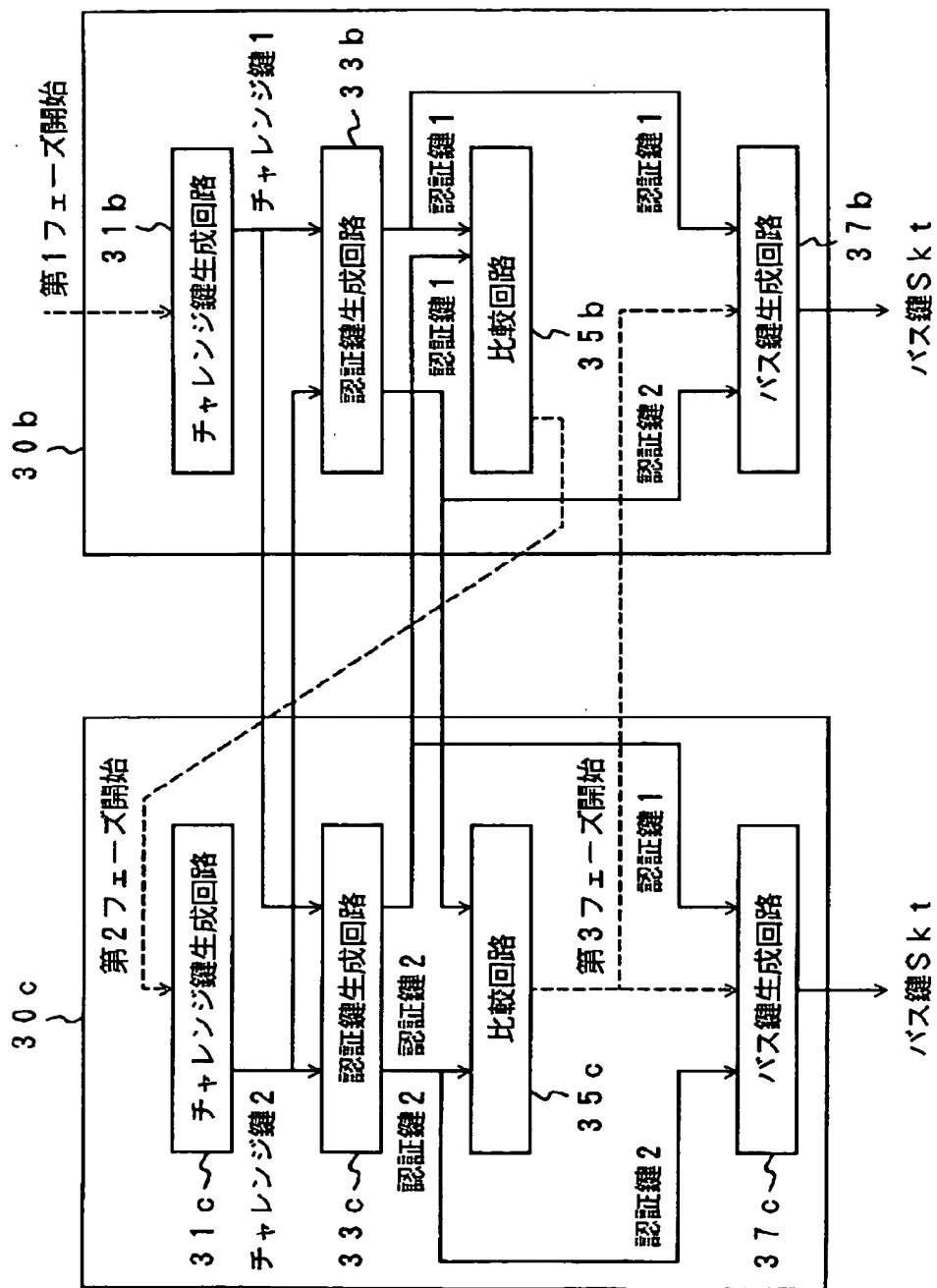
203…復号化ユニット

211、313…一時鍵判定回路

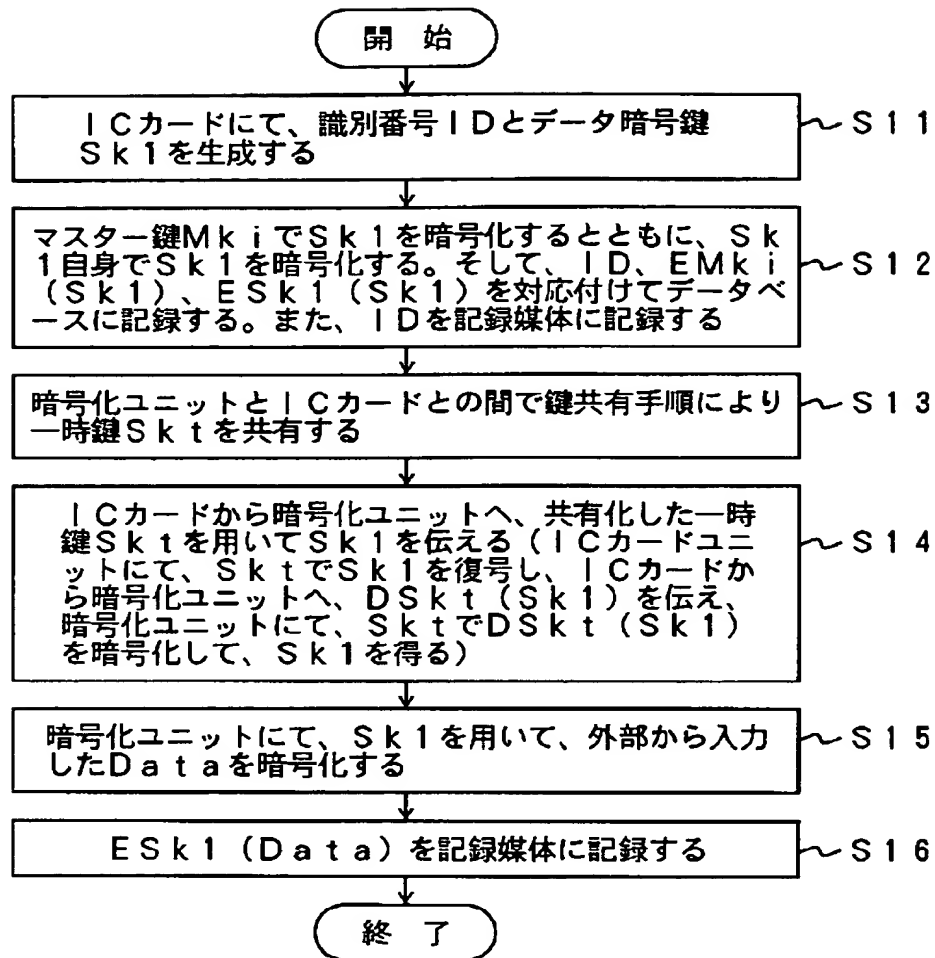
【図1】



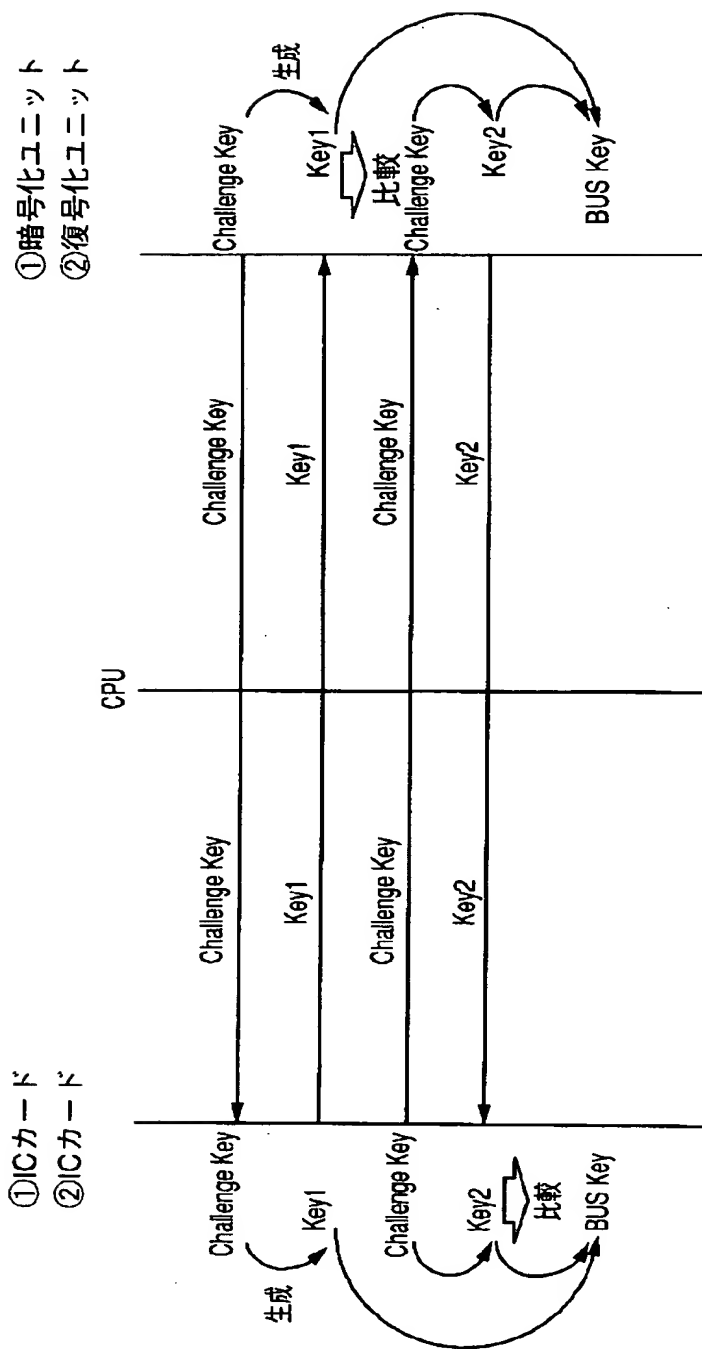
【図2】



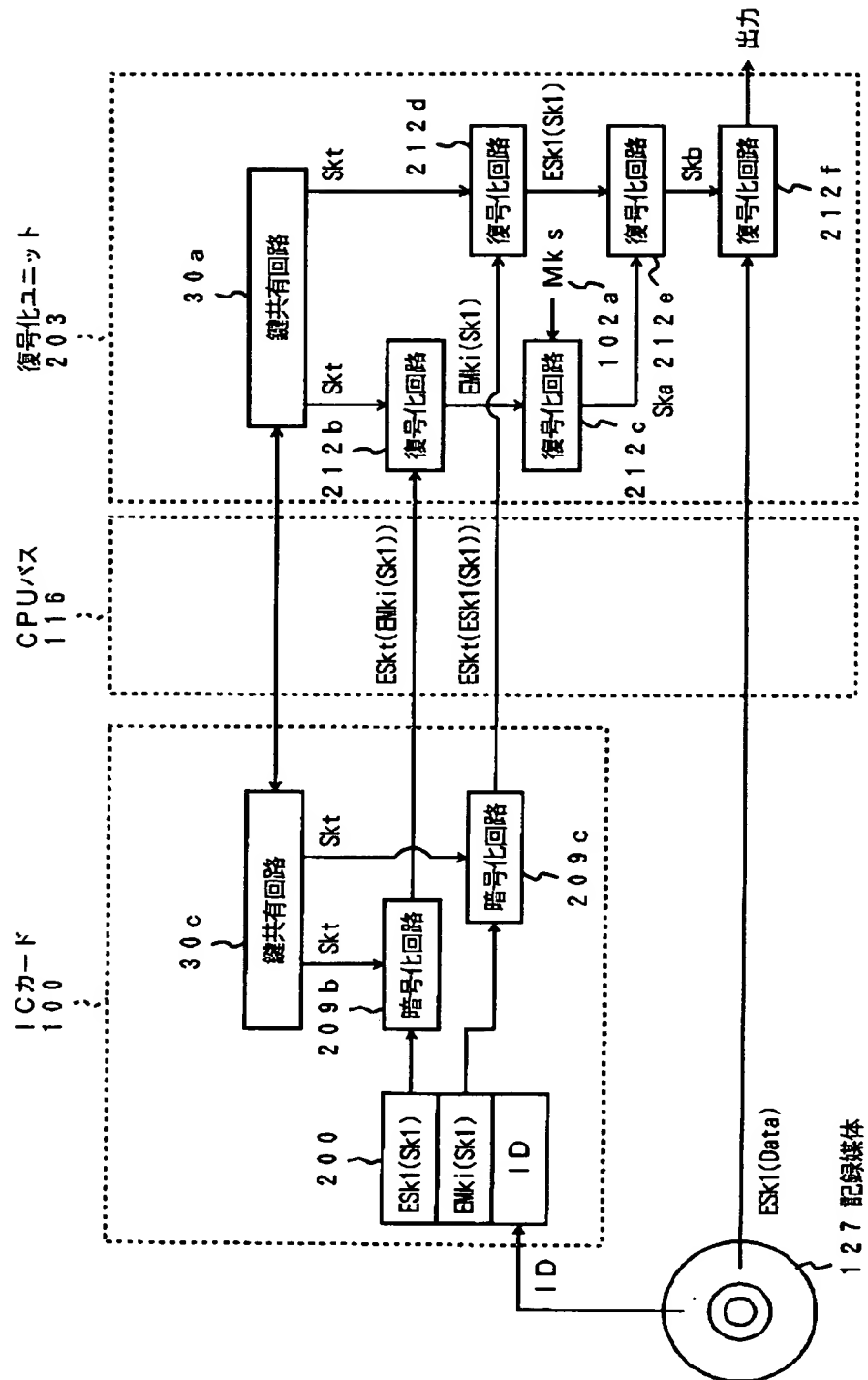
【図3】



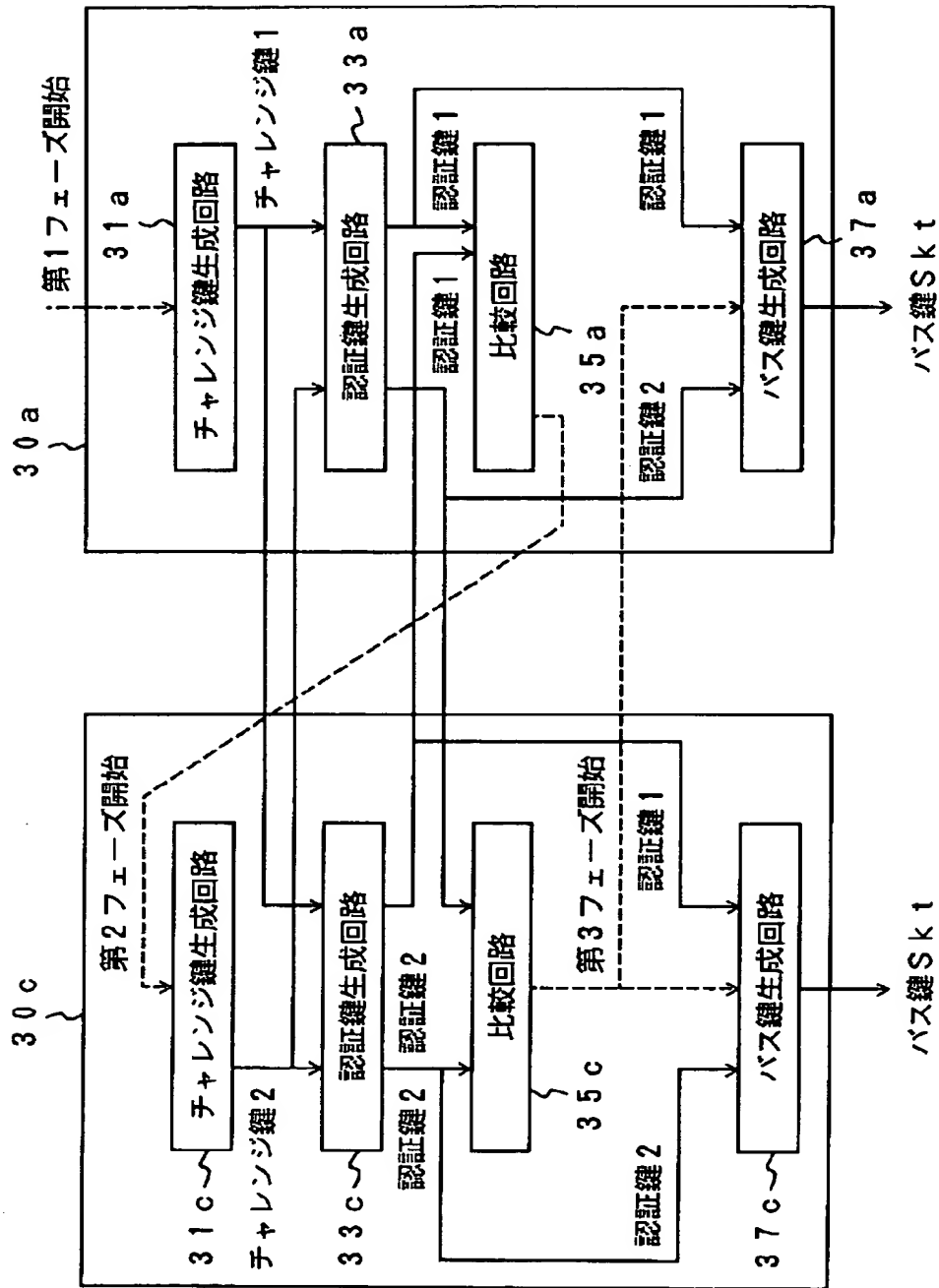
【図4】



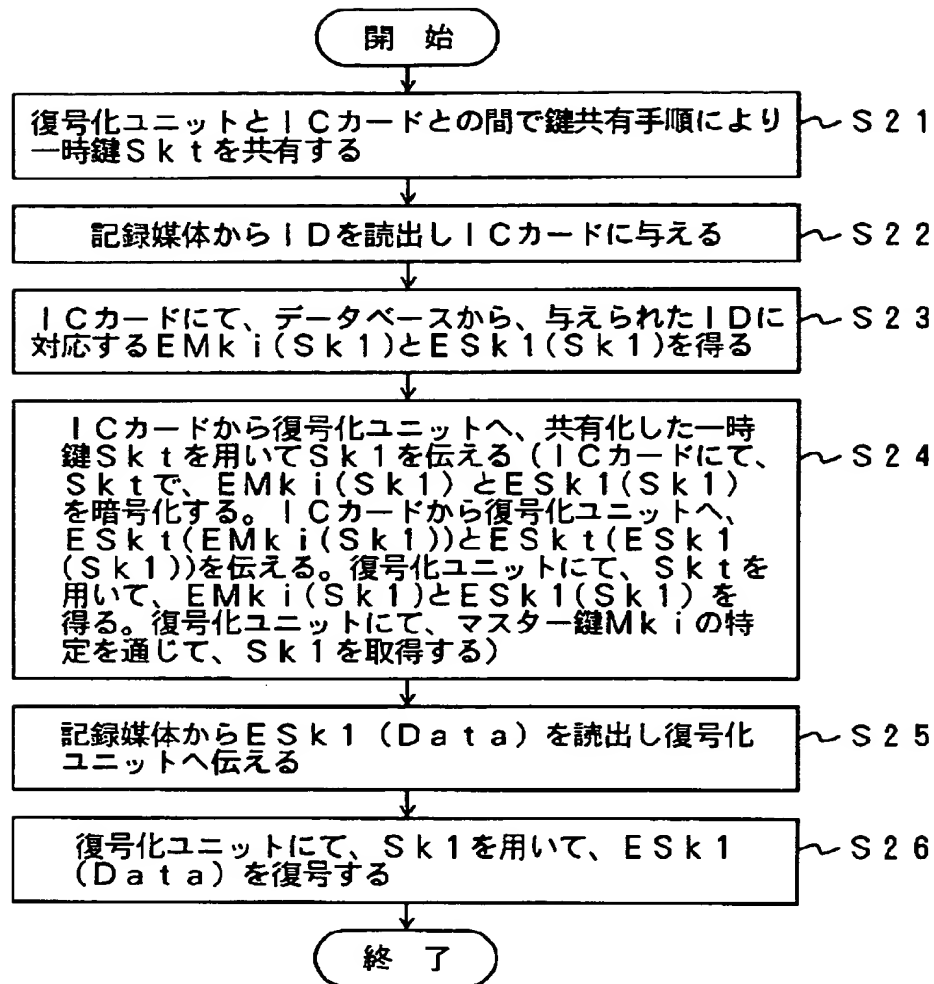
【図5】



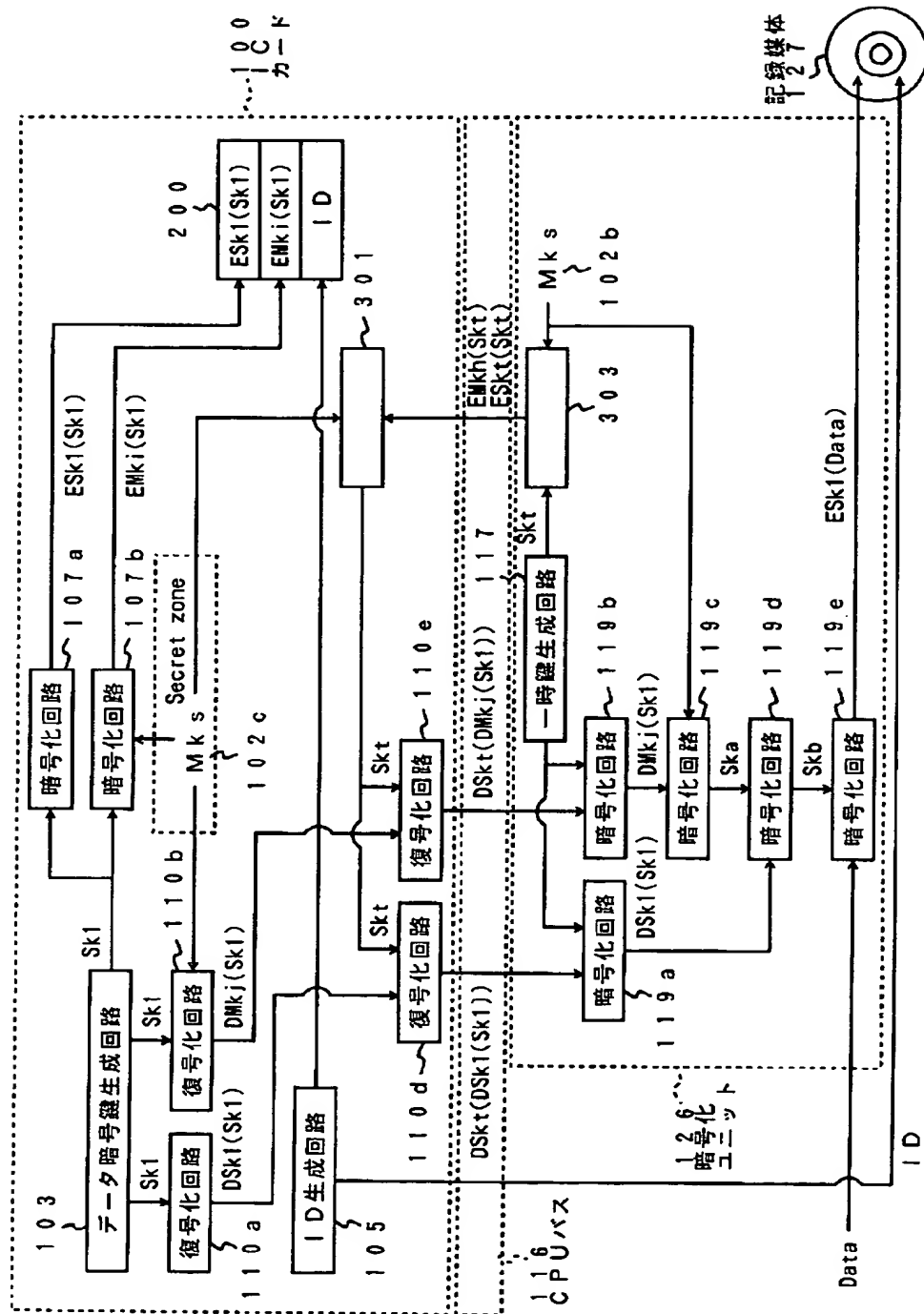
【図6】



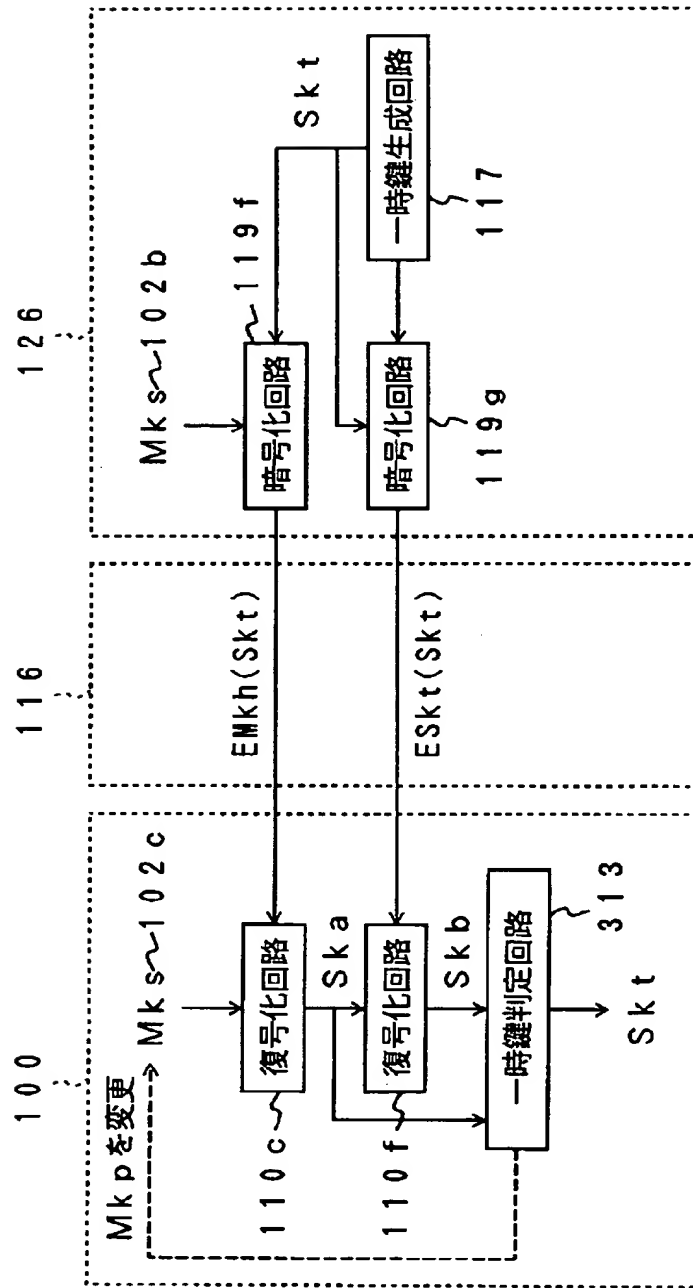
【図7】



【図8】



【図9】



【図10】

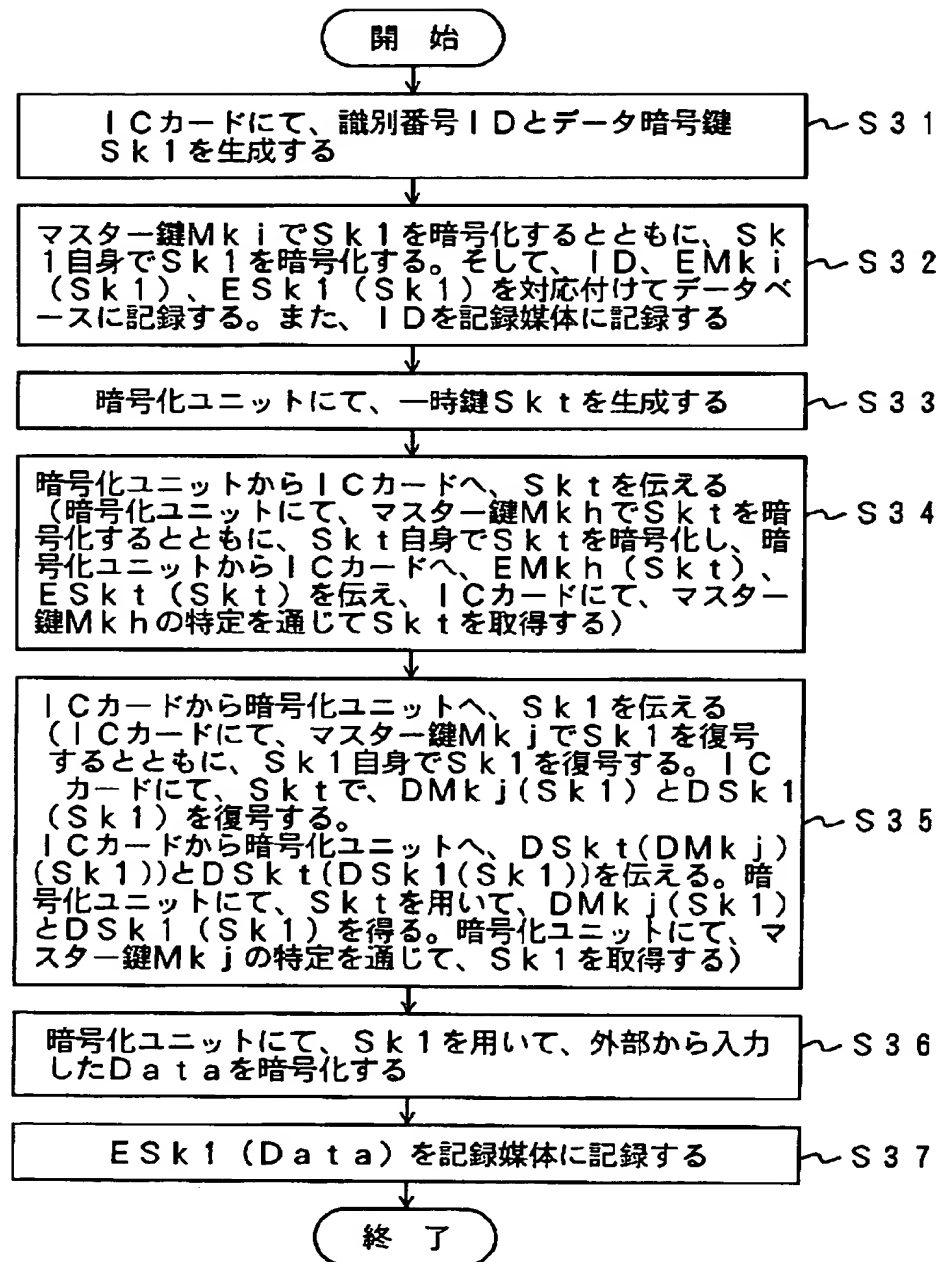
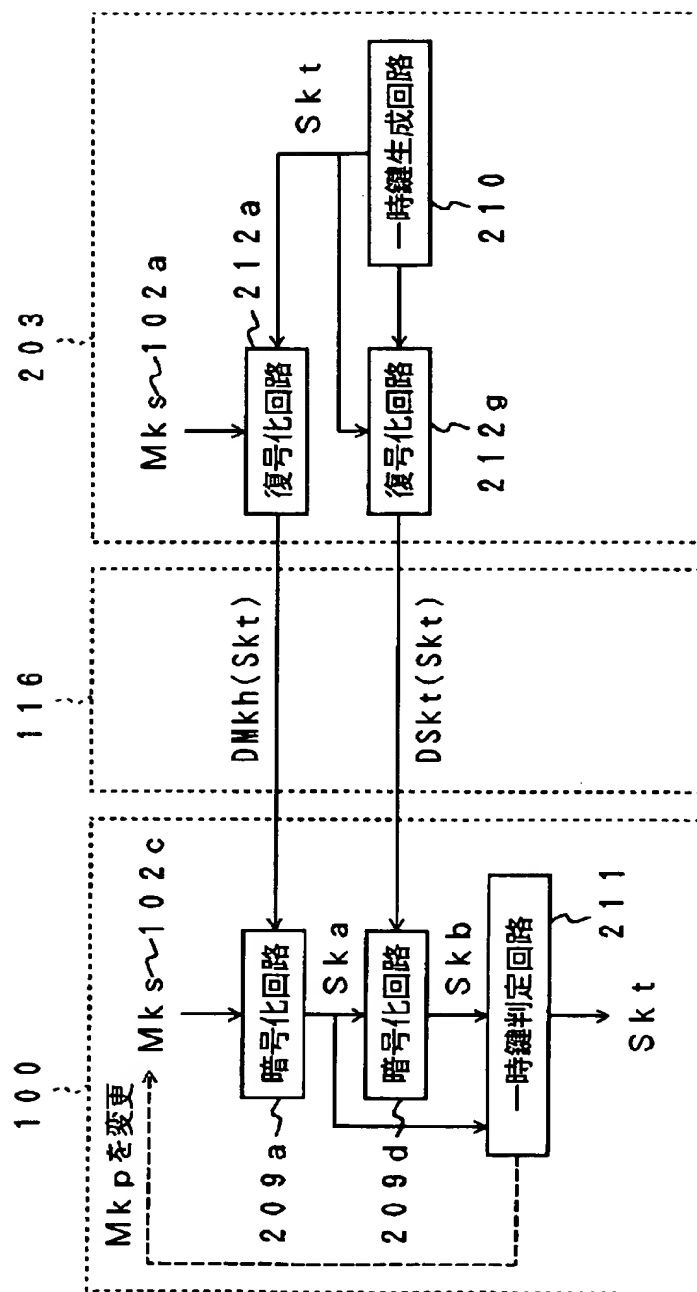
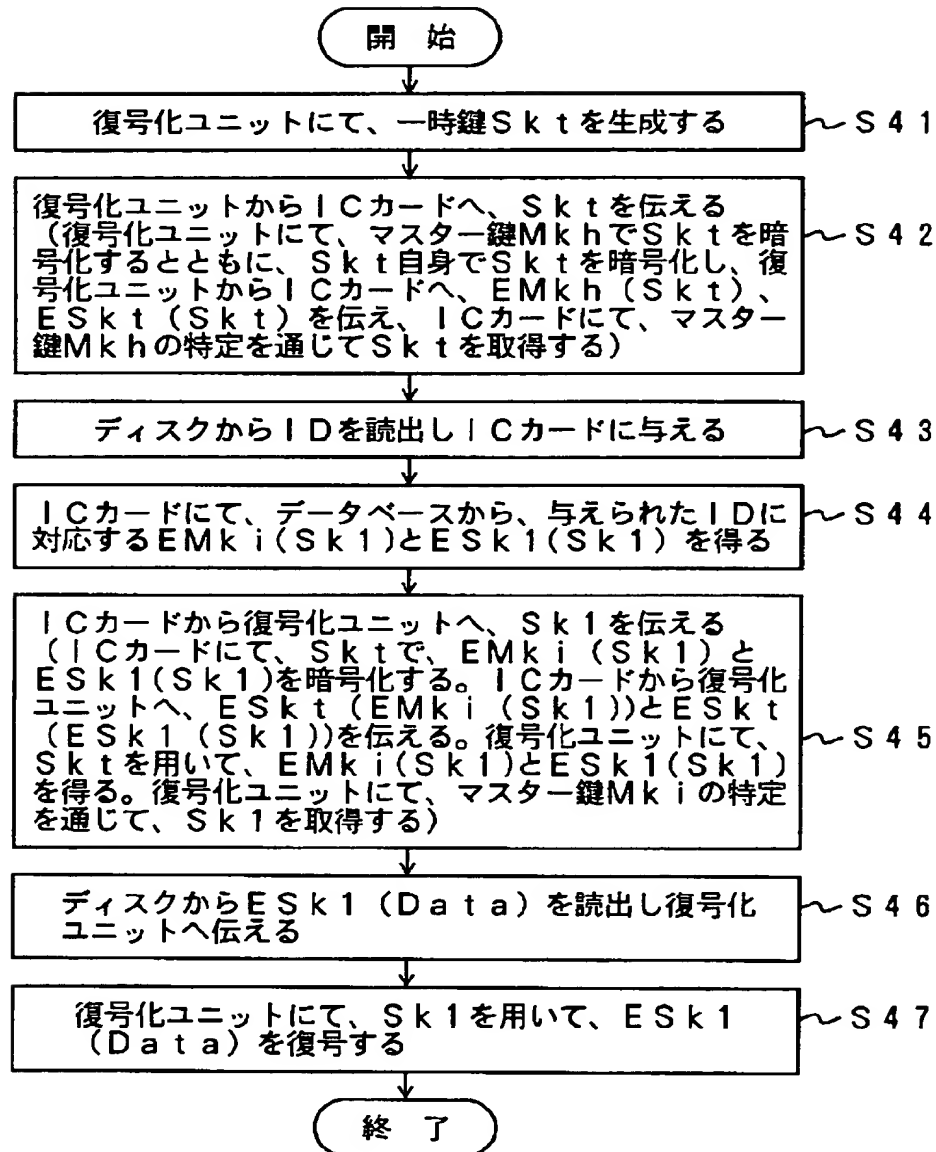


Figure 1 is a block diagram of a recording medium system. The system is divided into two main sections: the IC card (100) and the recording medium (127). The IC card (100) contains a CPU (116) and a secret zone (102c) which stores a master key (Mks) and a secret key (Skt). The recording medium (127) contains a CPU (203) and a secret zone (200) which stores a master key (Mks) and a secret key (Skt). The IC card also includes a one-time key generation circuit (210) and a decryption circuit (212d). The recording medium includes a decryption circuit (212b), a decryption circuit (212c), a decryption circuit (212e), and a decryption circuit (212f). The IC card outputs data (Esk1(Data)) to the recording medium.

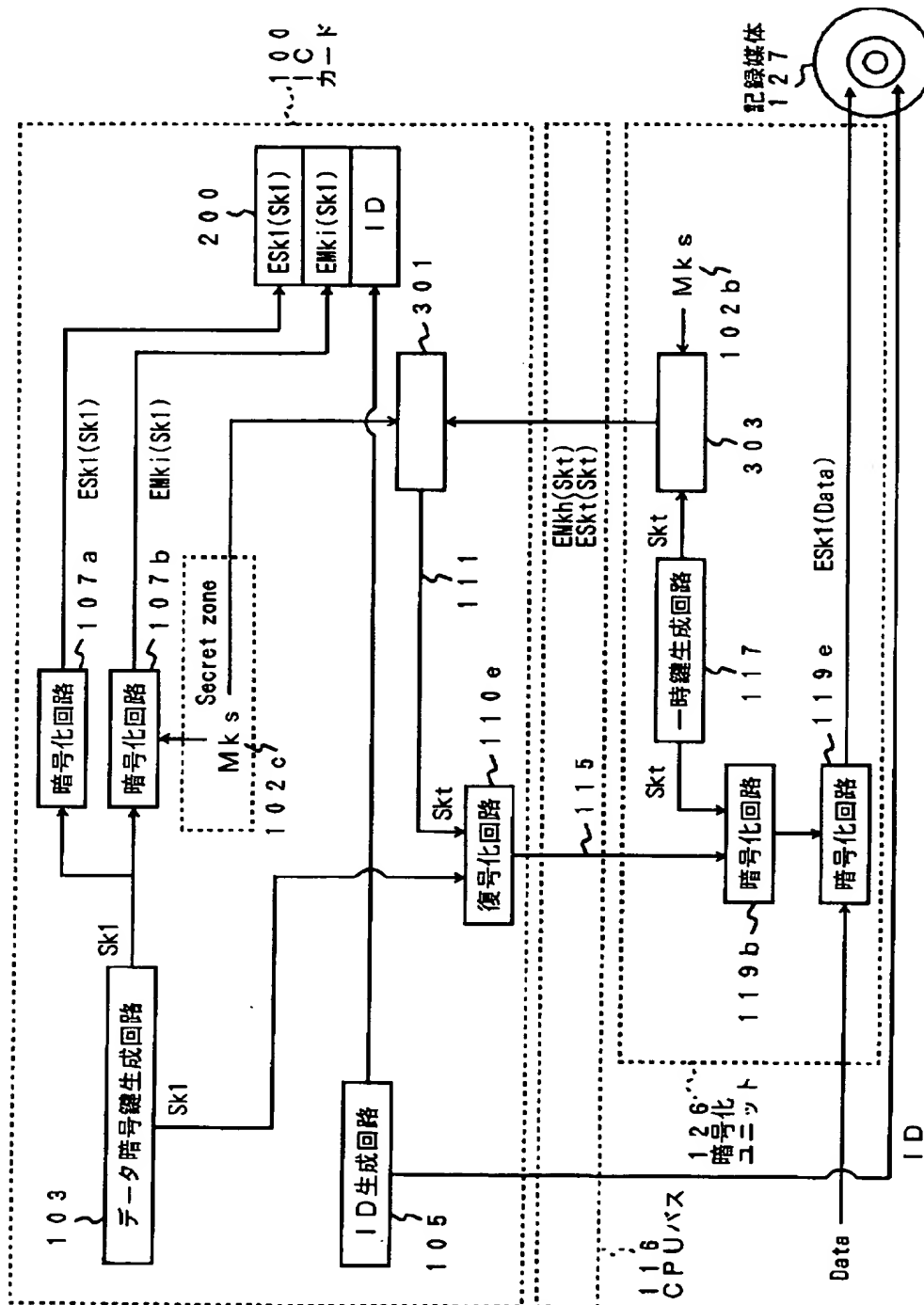
【图 1 2】



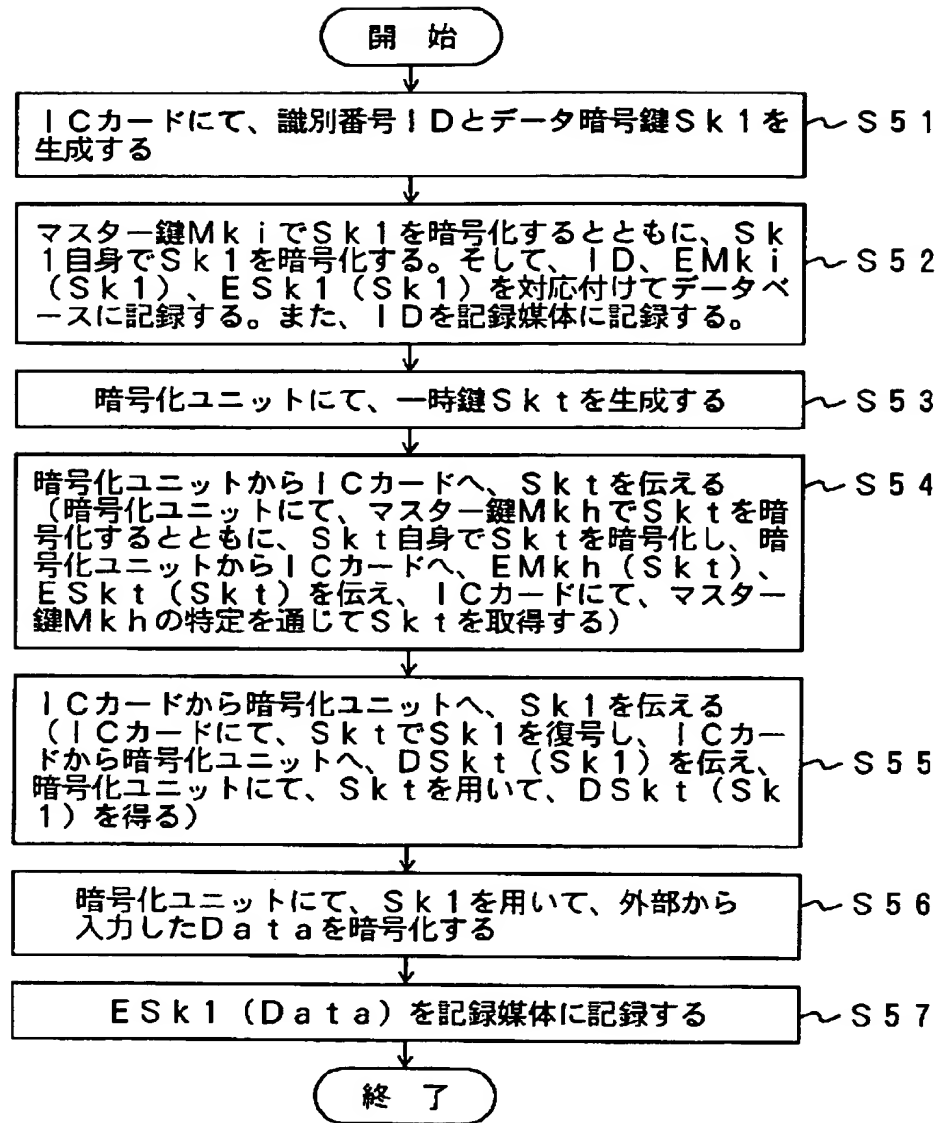
【図13】



【図14】



【図15】



フロントページの続き

(72)発明者 吉田 信博
 東京都青梅市末広町2丁目9番地 株式会
 社東芝青梅工場内